دراسات عالمية



حوكمة الإنترنت
في عصر انعدام الأمن الإلكتروني

روبرت كنيك



مركز الإمارات للدراسات والبحوث الاستراتيجية

العدد 95

حوكمة الإنترنت
في عصر انعدام الأمن الإلكتروني

مركز الإمارات للدراسات والبحوث الاستراتيجية

أنشئ مركز الإمارات للدراسات والبحوث الاستراتيجية في أبوظبي بتاريخ 14 آذار/ مارس 1994، كمؤسسة بحثية مستقلة تعنى بدراسة القضايا الاستراتيجية السياسية والاقتصادية والاجتماعية والمعلوماتية، التي تهم دولة الإمارات العربية المتحدة ومنطقة الخليج العربي خصوصاً والعالم العربي عموماً، ومتابعة أهم المستجدات الإقليمية والدولية.

وفي إطار التفاعل الثقافي والتعاون العلمي، يصدر المركز سلسلة **دراسات عالمية** التي تعنى بترجمة أهم الدراسات والبحوث التي تنشر في دوريات عالمية مرموقة، وتتصل موضوعاتها باهتمامات المركز العلمية، كما تهتم بنشر البحوث والدراسات بأقلام مشاهير الكتاب ورجال السياسة.

ويرحب المركز بتلقي البحوث والدراسات المترجمة، وفق قواعد النشر الخاصة بالسلسلة.

دراســات عـالميــة

حوكمة الإنترنت في عصر انعدام الأمن الإلكتروني

روبرت كنيك

العدد 95

تصدر عن





محتوىٰ الدراسة لا يعبر بالضرورة عن وجهة نظر المركز

This is an authorized translation of the Council Special Report no. 56 (September 2010), entitled "Internet Governance in an Age of Cyber Insecurity" by Robert K. Knake and published by Council on Foreign Affairs. The ECSSR is indebted to the author and to the publisher for permitting the translation, publication and distribution of this work under its name.

الطبعة الأولى 2011

ISSN 1682-1211

النسخة العادية ISBN 978-9948-14-412-0

النسخة الإلكترونية ISBN 978-9948-14-413-7

توجه المراسلات باسم رئيس تحرير سلسلة **دراسات عالمية**

على العنوان التالي:

مركز الإمارات للدراسات والبحوث الاستراتيجية

ص ب: 4567

أبوظبي، دولة الإمارات العربية المتحدة

هاتف: +9712-4044541

فاكس: +9712-4044542

E-mail: pubdis@ecssr.ae

Website: http://www.ecssr.ae

المحتويـات

تمهيد

أحدثت الإنترنت، منذ بدايتها عام 1989، ثورة في التجارة والاتصالات والعمل العسكري والحوكمة، ولم يعد من الممكن - ببساطة - تصور جزء كبير من العالم المعاصر من دونها، بيد أن تلك الثورة لم تكن من دون ثمن؛ فالتكلفة السنوية للجرائم الإلكترونية، [أو السبرانية؛ أي عبر الإنترنت]، تفوق الآن تريليون دولار، بينما شلَّت الهجمات الإلكترونية المنسَّقة، كلاً من: أستونيا وجورجيا وقرغيزستان، وألحقت الضرر ببنى أساسية حسّاسة، في دول مختلفة حول العالم، وبينما سعى ما لا يقل عن ستة من أجهزة الأمم المتحدة، والكثير من المنتديات الإقليمية والوطنية، للتوصل إلى توافق آراء، حول مستقبل حوكمة الإنترنت، [أو إدارتها]، فإنه لم يُحرَز إلا تقدم ضئيل في هذا المضمار حتى الآن، وقد امتنعت الولايات المتحدة الأمريكية بنفسها - إلى حد بعيد - عن هذه المناقشات، وركَّزت، بدلاً من ذلك، على تطوير قدراتها الهجومية والدفاعية، في مجال الأمن الإلكتروني، مع الاعتماد على خبرات القطاع الخاص؛ للمحافظة على استمرار استقرار النظام.

يتفحص روبرت كنيك، في هذا التقرير، القرارات التكنولوجية التي أتاحت النجاح الباهر للإنترنت، وجعلتها - في الوقت ذاته - عرضة للهجمات، على نحو يثير القلق! ويرى المؤلف أن الولايات المتحدة، لم يعد بإمكانها أن تتخلى عن زمام المبادرة، في المسائل الإلكترونية، لمصلحة دول لا تشاركها المصالح، ويرسم المؤلف الخطوط العريضة، للأجندة التي يمكن أن تسعى لتحقيقها، بالتنسيق بينها وبين حلفائها على الصعيد الدولي، ويضيف: أن تلك الأجندة - وهي التي تعالج مسائل الحرب الإلكترونية، والجريمة الإلكترونية، والتجسس الذي ترعاه الدول - ينبغي السعي لتحقيقها، باستخدام الأساليب التكنولوجية والقانونية معاً، وهو يحثّ الولايات المتحدة على أن تبدأ بدعم الخبراء، بما يمكّنهم من التصدي للمسائل الأمنية الأساسية التي تكمن في صلب تصميم الإنترنت، ثم يحدد الأدوات القانونية الضرورية؛ لمعالجة مسألتي: الجريمة الإلكترونية، والنشاطات التي ترعاها الدول؛ ومن ذلك: تدابير منع الجريمة الإلكترونية، على المستوى

الوطني، والآليات المتعددة الأطراف؛ لمنع الهجمات الإلكترونية، وملاحقة مرتكبيها، وقواعد حماية النظم المدنية الحساسة في زمن السلم، ويصف - من بعد ذلك - الإصلاحات البيروقراطية التي يتعين على الولايات المتحدة القيام بها؛ للتنفيذ الفعّال لتلك التغييرات.

وتقرير **حوكمة الإنترنت في عصر انعدام الأمن الإلكتروني**، إسهام يأتي في حينه، حول مسألة، تستحوذ بصورة متزايدة، على اهتمام صانعي السياسات، وهو يقدِّم أفكاراً تقنية لغير الخبراء، بلغة سهلة وجذابة، والتقرير لا يَدَع مجالاً للشك، في أهمية الأمن الإلكتروني، بالنسبة إلى مستقبل الولايات المتحدة، ومستقبل الإنترنت ذاتها، وتوفِّر توصياته، أساساً قوياً، يُستند إليه، إزاء ما سيتم اتخاذه من تدابير في المستقبل.

ريتشارد هاس

رئيس مجلس العلاقات الخارجية

أيلول/ سبتمبر 2010

كلمة شكر

لم يكن هذا التقرير ليرى النور؛ لولا استفادته من الخبرة والمشورة والصبر لدى لجنته الاستشارية؛ ذلك أن كل عضو من أعضائها، لديه من الخبرة في هذه المسائل، ما يفوق بكثير إسهامي في هذا المشروع، وأنا أدين لهم بالعرفان؛ لقبولهم إتاحة الاستفادة من تلك الخبرة، وتحمُّلهم عناء قراءة المسودات الكثيرة للتقرير، وأما الأخطاء الوقائعية أو المنطقية، وهي التي قد تكون ماتزال قائمة، فإنها تعود مسؤوليتها إلي وحدي.

فقد أدّت إستر دايسون، مهمة رائعة، من خلال ترؤسها اجتماعات اللجنة الاستشارية، وإتاحتها - في الوقت ذاته - الاستفادة من آرائها النقدية، والخبرة التي اكتسبتها، على مدى عقود، داخل مجتمع حوكمة الإنترنت، وأدين بالشكر لريتشارد هاس، رئيس مجلس العلاقات الخارجية، وللجنة جمعية الشؤون الخارجية بالمجلس؛ للفرصة التي مُنحتها؛ كي أمضي عاماً من العمل، على وضع سياسة، إزاء ما يخصّ الأمن الإلكتروني، والشكر موصول - أيضاً - إلى جيمس ليندسي، النائب الأول لرئيس المجلس، ومدير الدراسات، وأستاذ كرسي موريس آر جرينبرج؛ للدعم الذي شمل به المشروع، إلى أن رأى النور؛ وللصبر الذي تحلّى به، لدى مراجعة مسودات عدّة، إلى أن اتضحت اللغة، واستبانت المصالح القومية للولايات المتحدة.

وقد وفّر لي برنامج الشركات،* وبرنامج الكونجرس** للمجلس، الفرصة؛ كي اختبر الأفكار المتضمَّنة في هذا التقرير، في حضور لفيف من الخبراء، قبل نشره؛ فتحسَّن التقرير كثيراً؛ بفضل التعليقات التي تلقّيتها في كل جلسة، وقد دعاني جيمس لويس، من مركز الدراسات الاستراتيجية والدولية، إلى المشاركة في اجتماعات مع معهد العلاقات الدولية المعاصرة في الصين؛ حيث اكتسبت فهماً قيّماً مباشراً، لأهداف ذلك البلد، وغاياته، على صعيد حوكمة الإنترنت.

---

* لقاءات تفاعلية بين أعضاء المجلس وقادة الأعمال والمال بشأن التحديات الدولية المهمة. (المترجم)

** ملتقيات إحاطة ونقاش مع أعضاء الكونجرس وصانعي السياسات في واشنطن. (المترجم)

وأودّ أن أتوجه بالشكر، لجون رولينز، في قسم أبحاث الكونجرس؛ لمساعدتي على فهم دور الكونجرس في حوكمة الإنترنت، ولفينس كريسلر، من شركة زايكنر ريسك آناليتيكس المحدودة؛ لتقديمه فهماً قيّماً لتحديات السياسات، ومشورة تقنية، كنت أحوج ما أكون إليها، بشأن الآليات الداخلية للإنترنت، كما أشعر بالامتنان - كذلك - نحو رود بِكستروم، رئيس شركة الإنترنت للأسماء والأرقام المخصصة (ICANN)، وهو الذي حضر اجتماعنا الاستشاري الأول، في إطار اللجنة، وأطلعنا على تصوّره، وقد وافاني آدم سيجال، وهو زميل أول بالمجلس، بتقويماته باستمرار، وخصَّص جزءاً من وقته؛ لمساعدتي على إعادة تنظيم المسودة النهائية للتقرير، وعلى التركيز على المصالح القومية الأمريكية، في الفضاء الإلكتروني، والسبل المثلى لتحقيقها.

وأسهمت بريتي باتاشارجي، وهي باحثة مشاركة، في ضمان استمرار تقدُّم المشروع واكتماله، في الوقت المحدد، من خلال العناية بالتفصيلات كافة، على الوجه الأكمل، وساعدت لوسي داندرديل، وهي منسّقة الاتصال، على توجيهي، في أجواء مرحة، عبر مرحلة اعتماد التقرير، وساعدتني ريتشل هاريس، وهي متدربة سابقة في المجلس، على إجراء الأبحاث اللازمة؛ حيث عالجت بمهارة، طلبات صعبة، حول موضوعات غير شائعة.

وقد أُعدّ هذا التقرير، في إطار برنامج المؤسسات الدولية والحوكمة العالمية، الذي يقوده ستيوارت إم باتريك، وهو زميل أول؛ فقد قدَّم مشورة قيّمة، حول محتوى التقرير وبنيته، والمشروع أمكن تنفيذه؛ بفضل هبة سخية مقدَّمة من مؤسسة روبينا.

روبرت كنيك

مقدمة

لم تعد الولايات المتحدة، تتصدر الملتقيات الدولية التي ستحدد مستقبل الإنترنت؛ فالأنظمة غير الديمقراطية، بقيادة روسيا والصين، بدأت تنظم صفوفها؛ لتشكِّل جبهة موحدة تروِّج لرؤيةٍ للإنترنت، تتسم بإحكام الدول سيطرتها عليها، وهذه الرؤية تزداد جاذبيتها، لدى الكثير من الدول الأوربية التي تسعى جاهدة، لمعالجة تهديدات مترابطة، وممثلة بالجريمة الإلكترونية، والجاسوسية الصناعية، والحرب الإلكترونية، وعلى الولايات المتحدة، أن تكافح تلك التهديدات بنشاط، في الوقت الذي تعمل فيه، على حماية المصالح القومية الأمريكية المثلة بالمحافظة على الإنترنت، وتوسيع نطاقها؛ بوصفها منصةً لزيادة الكفاءة والتبادل الاقتصادي، وحماية هذه المصلحة، تتطلب تواصلاً أوسع بكثير، ضمن ملتقيات حوكمة الإنترنت؛ لتشكيل مستقبل الشبكة، على نحو يبدد الهواجس الأمنية، من دون أن يتمخض عن دواء أسوأ من الداء.

وتحقيقاً لهذا الهدف، فإن على الولايات المتحدة، أن تسترشد بمبادئ ثلاثة: أولاً، عليها أن تعتمد "نهجاً شبكياً وموزَّعاً" لـ "مشكلة شبكية وموزَّعة"؛ لأنه ما من منتدى، يمكنه أن يعالج [وحده] هذه المجموعة من المسائل، وعلى الولايات المتحدة الأمريكية أن تسعى - بدلاً من ذلك - لإيجاد حلول، من خلال مشاركة واسعة النطاق، تشمل مجموعة عريضة من المنتديات، وعلى الولايات المتحدة ثانياً، أن تتحرك باتجاه مساءلة الدول عن تصرفاتها وتصرفات مواطنيها وأنظمتها في الفضاء الإلكتروني؛ فمع أن الولايات المتحدة، لا يجوز أن تتوقع أن تمنع الدولُ كل أشكال السلوكيات الخبيثة، فإن لها أن تتوقع أن تتولى تلك الدول، حماية شبكاتها بدرجة معقولة، وسنّ القوانين التي تعاقب الجريمة الإلكترونية الدولية، وإرساء الآليات التي تستجيب لطلبات المساعدة على إحباط الهجمات، والتحقيق فيها، وملاحقة مرتكبيها، وعلى الولايات المتحدة ثالثاً، أن تكون القدوة؛ إذ عليها أن تتخذ خطوات؛ لتنظيف شبكتها القومية، والحيلولة دون أن تُستغل أنظمتها في الهجمات الإلكترونية الدولية، ومنح التحقيقات الجنائية في الهجمات الإلكترونية مع الضحايا الأجانب الأولوية، وإيضاح أن الهدف الأساسي من جهودها العسكرية، في الفضاء الإلكتروني، إنما هو حماية الولايات المتحدة، والمحافظة على التواصل الدولي.

وهذه الأهداف، يجب تطبيقها، ضمن جدول ثلاثي الأجزاء؛ فالولايات المتحدة، عليها أن تعمل على تطوير مجموعة نظم دولية أقوى؛ لمكافحة الجريمة في الفضاء الإلكتروني؛ بما يتعدى اتفاقية مجلس أوربا الراهنة، [وهي الخاصة بالجرائم الإلكترونية]؛ لاستقطاب الدول غير الغربية، واستحداث آليات، تعمل في الوقت الحقيقي؛ [أي على الفور]؛ للتعاون على وقف الهجمات الإلكترونية الجارية، والتحري عن الهجمات عبر الحدود، بيد أن معالجة الجريمة الإلكترونية وحدها، لا تكفي لتأمين الفضاء الإلكتروني؛ فالدول يجب تقييدها - كذلك - من خلال استحداث قواعد جديدة، وليس على الولايات المتحدة أن تخشى الحديث عن هذه الموضوعات، بل عليها أن تبرم اتفاقيات؛ لحماية الوظائف الأساسية للإنترنت، ومنع هجمات حجب الخدمة الموزَّعة،* وعليها - أيضاً - أن تحيي الجهود؛ لتأمين التكنولوجيات الأساسية للإنترنت، وهي التي طُوِّرت قبل عقود؛ لغرض يختلف عن الغرض الذي تُستخدم اليوم من أجله.

وعلى الولايات المتحدة أخيراً، أن ترسي آليات ضمن حكومتها؛ لتحقيق تلك الجداول، وهناك حاجة إلى مستوى قيادة أقوى في البيت الأبيض؛ لضمان استمرار التركيز على المصالح القومية الأمريكية، من الوكالات المهتمة بكيفية تطوير الإنترنت، ولا بد من الارتقاء بمسألة حوكمة الإنترنت لدى وزارة الخارجية، بحيث يُعنى بها مكتب جديد، يركز على الشؤون الإلكترونية؛ على أن توكل إليه مهمة العمل؛ لتحسين أمن الفضاء الإلكتروني، من خلال المشاركة الدولية، كما يجب أن يُفسَح المجال أكثر، للقطاع الخاص؛ كي يبدي رأيه بشأن تلك الموضوعات والآليات التي يتم تطويرها؛ من أجل الشركات؛ كي تسهم في تشكيل السياسة الأمريكية، وتنسِّق مواقفها.

* أحد أشكال تلك الهجمات، إغراق الهدف - (وهو أحد المواقع الشبكية مثلاً) - بطلبات الاتصال الخارجية؛ فيؤدي هذا إلى عجزه عن الاستجابة، أو الاستجابة ببطء، بحيث يعد غير متاح. (المترجم)

معلومات أساسية

منذ الأيام الأولى للإنترنت، سعى أبرز مصمميها ومؤيديها، للحدّ من دور الحكومة، في تصميم الشبكة وعملها وإدارتها، ومع أن الإنترنت نتاج أبحاث، موَّلتها الولايات المتحدة طوال عقود، فإن علماء الحاسوب الذين طوروا البروتوكولات التي تعمل الإنترنت؛ وفقها اليوم، صمَّموها، بحيث لا توجد ضرورة لمشغِّل مركزي للشبكة، وطوال العقود الثلاثة السابقة، نجحت إدارات رئاسية متعاقبة، في اعتماد نهج، يقوم على عدم التدخل في تطوير الشبكة؛ فيسمح هذا للإنترنت بالنمو من دون مشاركة حكومية، كان يمكنها أن تحدّ من توسعها المطّرد أو توقفه، وقد تم توسيع نطاق هذا النهج؛ ليشمل المشهد الدولي ككل؛ حيث حافظت الولايات المتحدة على السيطرة على مكوّن ضروري واحد من مكونات البنية الأساسية للإنترنت، تتعين إدارته بنشاط؛ أي نظام اسم النطاق Domain Name System، وأما ماعدا ذلك، فكان موقفها يقوم على أن دور الحكومات في إدارة الشبكة، يجب أن يبقى محدوداً؛ وقد أدّى ظهور الجريمة الإلكترونية، والتجسس الإلكتروني، وشبح الحرب الإلكترونية، إلى أن تمارس حكومات أجنبية كثيرة، السلطة السيادية على شبكاتها، وتضغط على المنظمات الدولية؛ كي تُعنى بتلك المسائل.

فهم التهديد

يُقدَّر الضرر الذي تلحقه الجريمة الإلكترونية بالاقتصاد العالمي، بما يزيد على تريليون دولار سنوياً؛[1] فالهجمات المتطورة التي تستهدف الملكية الفكرية، لشركات [مجلة] **فورتشن 500**، أصبحت من الأمور الروتينية، وقد انخرطت الدول في المشهد الممتزج؛ حيث طوَّرت قدرات هجومية ودفاعية معاً، ضمن شكل جديد من أشكال سباقات التسلح، والولايات المتحدة، في طريقها إلى تدشين القيادة الإلكترونية، وهي قيادة قتالية جديدة، يوكل إليها الإشراف على العمليات الهجومية والدفاعية، في الفضاء الإلكتروني، ويترأسها جنرال بأربعة نجوم، وهناك أربع دول أخرى على الأقل، طوَّرت قدرات على القيام بعمليات إلكترونية هجومية متطورة، بينما شرع ما يزيد على مائة دولة، في تنظيم وحدات للحروب الإلكترونية.[2]

وتلك القدرات، لم تكن مقصورة على المختبرات؛ ففي عام 2007، تعرضت أستونيا لهجوم حجب الخدمة على المستوى الوطني؛ أدّى إلى أن يبقى البلد كله، مفصولاً عن الإنترنت على مدار أسبوع؛ فأثّر هذا في: الشبكات الحكومية، وشبكات الاتصالات، والدوائر المالية،[3] وبعد مضي عام، وعندما غزت روسيا جورجيا، سبق هجومٌ في الفضاء الإلكتروني القوات البرية والجوية، وتلك الصراعات المبكرة في الفضاء الإلكتروني، إنذارات محتملة بهجمات، أسوأ بكثير، وقد برهن الباحثون على القدرة على استخدام الهجمات الإلكترونية؛ لتدمير القيود المالية، وقطع التيار الكهربائي، وتعطيل الشبكات الضرورية للعمليات العسكرية، وأصبحت قطاعات رئيسية في مجال البنية الأساسية - ومنها قطاعات: الطاقة والنفط والغاز والمياه والصرف الصحي - مستهدفة على نحو متزايد.[4]

حوكمة الإنترنت اليوم

إن الإنترنت؛ بوصفها شبكة مؤلفة من شبكات، لا تخضع لسلطة مركزية،[5] والمعايير التقنية الجديدة للبروتوكولات التي تعمل الإنترنت وفقها، يتم تطويرها من خلال عملية "طلب تعليق"* تكرارية، تديرها فرقة العمل المعنية بهندسة الإنترنت،** ويعتمدها المجتمع التقني على أساس توافقي؛ وإدراكاً للحاجة إلى سلطة مركزية؛ لتخصيص معرِّفات identifiers، اسمية ورقمية فريدة، استحدث نظام اسم النطاق، في أوائل الثمانينيات من القرن العشرين، والدور الممثل بتخصيص عناوين بروتوكولات الإنترنت، وإدارة منطقة الجذر root zone: (أسماء وعناوين لبروتوكولات الإنترنت الخاصة بخوادم نظام أسماء النطاق المعتمدين أو المخوَّلين لجميع نطاقات المستوى الأعلى؛ من قبيل: "دوت كوم".com)، كان يضطلع به فرد واحد، يُدعى جون بوستل John Postel، مدة تقارب العقدين،[6] وفي عام 1998، استحدثت وزارة التجارة الأمريكية، شركة الإنترنت للأسماء والأرقام المخصصة ICANN؛ للإشراف على إدارة هذا النظام من المعرِّفات الفريدة.

---

* مذكرة تصدرها فرقة العمل المعنية بهندسة الإنترنت، تصف فيها: الأساليب أو السلوكيات أو الأبحاث أو الابتكارات التي يمكن تطبيقها، على عمل الإنترنت والنظم المتصلة بها. (المترجم)

** المنظمة الرئيسية المعنية بوضع المعايير الخاصة بالإنترنت، وهي مجتمع دولي كبير مفتوح، من المصممين والمشغّلين والباعة والباحثين المعنيين بتطوير بنية الإنترنت، وعملها بشكل سلس. (المترجم)

وتشغِّل شركة ICANN، النظام المركزي الوحيد الضروري لاستمرار عمل الإنترنت، وهي تضطلع بذلك الدور، بحجم تكلفة أدنى، وتتخذ التدابير؛ لمعالجة المسائل الأمنية التي تدخل ضمن نطاق ولايتها، ويرى الكثير من رواد الإنترنت ومن مؤيدي حريتها، أن تخصيص تلك المعرِّفات الفريدة، هو الوظيفة الضرورية الوحيدة، على صعيد حوكمة الإنترنت، وقد اتفقت إدارات أمريكية متعاقبة إلى حد كبير على هذا الرأي، وحدَّت من تدخل الحكومة الأمريكية، وسعت لكبح حكومات أخرى، إزاء محاولة ممارسة السلطة على الشبكة، بما يتيح للشبكة أن تنمو من دون عوائق، بيد أن الاتجاه المتصاعد للبرمجيات الضارة، وانتشار سرقات الهوية والجرائم المالية، واستخدام الإنترنت من الإرهابيين، والمستويات غير المسبوقة التي بلغها التجسس بين الشركات، وتطوُّر قدرات الدول في مجال الحرب الإلكترونية الهجومية، والاستغلال الإلكتروني، كلها عوامل، تشير إلى الضرورة المحتملة لنمط حوكمة أقوى وأشمل؛ كي تنمو الإنترنت، وتواصل إضافة قيمة إلى التجارة العالمية، وجعل الحياة اليومية للمليارات من البشر ثرية.

وبالنظر إلى تكاليف الجريمة والتهديد الاقتصادي للتجسس الصناعي وتزايد عسكرة الفضاء الإلكتروني، فإن نهج عدم التدخل الذي كانت الولايات المتحدة، تعتمده بشأن حوكمة الإنترنت، طوال العقد الماضي، لم يعد من الممكن إدامته، وعلى الرغم من أن الإنترنت التي نعرفها اليوم، هي نتاج مجهود تعاوني بين الحكومة الأمريكية، والقطاع الخاص، والمجتمع الأكاديمي، فإن حق المباهاة المتأتي من ملكية السبق التاريخي، لا يمتد إلى السيطرة على مستقبل الإنترنت؛ فإذا لم تتحلَّ الولايات المتحدة بالقيادة الضرورية؛ لمعالجة المشكلات الأمنية، فإن دولاً أخرى سوف تتولى ذلك، وإذا كانت الإنترنت بصورتها الحالية، تجسيداً للانفتاح والابتكار اللذين يتّسم بهما المجتمع الأمريكي، فإن الإنترنت المستقبلية - وفق تصور روسيا والصين - سوف تجسّد مجتمعيهما؛ أي ستكون منغلقة، ومعتلّة، وخاضعة لسيطرة الدولة، وواقعة تحت مراقبة مكثفة.

مبادرات حكومية دولية جديدة

وبالنظر إلى الهواجس الأمنية، نجد أن بلداناً كثيرة، تتعجّل اعتماد مبادرات جديدة؛ بهدف تأمين الفضاء الإلكتروني، في عدد ضخم من المنتديات الدولية التي تتسابق على الاضطلاع بدور في حوكمة الإنترنت؛ ومن ذلك: ما لا يقل عن ستة منتديات داخل الأمم المتحدة وحدها، كما تنشط - كذلك - مجموعات إقليمية؛ مثل: رابطة التعاون الاقتصادي لآسيا والمحيط الهادي، ومنظمة التعاون الاقتصادي والتنمية، ومنظمة الدول الأمريكية، وتمارس الحكومة الروسية، ضغوطاً منذ عام 1998؛ للتوصل إلى معاهدة - ضمن إطار الأمم المتحدة - تعالج الصراع في الفضاء الإلكتروني، وقد بدأت الفكرة تكتسب زخماً في الآونة الأخيرة، كما حظي المفهوم بالتأييد، في مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، وهو الذي عُقد في سلفادور، بالبرازيل، في نيسان/ إبريل عام 2010،[7] ويبذل حامادون توري Hamadon I. Touré، وهو الأمين العام للاتحاد الدولي للاتصالات، جهداً حثيثاً؛ للوصول إلى مثل ذلك الاتفاق، وقد دعا مؤخراً، إلى عقد مؤتمر للأمم المتحدة، يتولى وضع "مخطط لنهج على نطاق المنظومة"، إزاء ما يتعلق بأمن الفضاء الإلكتروني.[8]

ومن الواضح أن هذه النتيجة، تتناقض والمصالح الأمريكية؛ فالاتحاد؛ بوصفه منظمة، ليس مصمَّماً لإدارة مسائل معقدة؛ مثل: أمن الفضاء الإلكتروني، وهو غير مكلف بمعالجة مسائل؛ مثل: الجريمة، والصراعات بين الدول، كما أن الاتحاد؛ بوصفه منظمة دولية حكومية، عمادها الدول، ليس مصمَّماً، بحيث تشارك المنظمات غير الحكومية والقطاع الخاص في مناقشاته، أما مقابلة زخم تلك المبادرة فتتطلب ما هو أكثر من تجاهلها أو معارضتها، وعلى الولايات المتحدة، أن تتعدى حدود وظائف شركة الإنترنت للأسماء والأرقام المخصصة، بحيث تعمل بروح من التعاون، مع دول أخرى؛ بغية استحداث آلية مثلى؛ للتنسيق الدولي؛ لمكافحة الجريمة الإلكترونية، ووضع قواعد الحرب في الفضاء الإلكتروني، والترويج لتطوير تشكيلة جديدة آمنة، من بروتوكولات الإنترنت.

إعادة النظر في المصالح الأمريكية في الفضاء الإلكتروني

إن المصلحة القومية الطاغية للولايات المتحدة، في الفضاء الإلكتروني، تكمن في المحافظة على الإنترنت، وتوسيع نطاقها؛ بوصفها أداةً من أدوات الكفاءة الاقتصادية، داخل الوطن، وعاملاً ميسِّراً للتبادل الاقتصادي على المستوى الدولي، أما المستوى الحالي للنشاط الإجرامي والتجسس وإعداد ساحة المعركة في الفضاء الإلكتروني، فيهدد بتعطيل المكاسب الاقتصادية المتأتية من التوصيل الشبكي للنظم، طوال العقدين الماضيين، إن لم يكن يمحو تلك المكاسب كلها، وعلاوة على ذلك، فإن المبالغة في الاستجابة لتلك التهديدات، قد تكون لها الآثار المدمرة ذاتها، وعلى الولايات المتحدة - لدى سعيها لتحسين الأمن في الفضاء الإلكتروني - أن تعمل؛ للمحافظة على ما للشبكة من خصائص أساسية، ترفع إلى حد كبير، من قيمتها بالنسبة إلى التبادل الاقتصادي؛ أي: الابتكار والانفتاح والحوكمة المحدودة، وهذه الخصائص تجعل الشبكة مرنة، بحيث يسهل تطوير الاستخدامات الجديدة، وقابلة للتطوير، بحيث يمكن توصيل ملايين المستخدمين والأجهزة، كل عام؛ فيوسِّع ذلك نطاقي التدفق الحر للأفكار، والتجارة الدولية، لكن معالجة مشكلات الأمن في الفضاء الإلكتروني، على حساب تلك الخصائص، لن تخدم المصالح القومية الأمريكية.

إن المكاسب الهائلة - على صعيد الإنتاجية الاقتصادية - طوال العقدين الفائتين؛ هي نتيجة للاستخدام المباشر الموسَّع للإنترنت، في: الاتصال والتعاون والتعهيد وإدارة المخزون في الوقت المناسب؛ [على أساس تقليل الفاقد]، ومراقبة العمليات الصناعية، وعلى الصعيد الدولي، نجد أن ما حدث من توسّع في التجارة العالمية، في السلع والخدمات معاً، لم يكن ليتحقق لولا الإنترنت؛ بوصفها تكنولوجيا ممكِّنة، والنشاط الخبيث في الفضاء الإلكتروني، يهدد تلك النظم؛ ففي مجال التجسس بين الشركات وحده، بدأ الكثير من هذه الشركات، يشكك في الحكمة من استخدام الإنترنت؛ للسماح بالاضطلاع بنشاطات البحث والتطوير، على مدار الساعة، وفي جميع المناطق الزمنية؛ بسبب فقدان حقوق الملكية الفكرية؛ نتيجة للهجمات.

والولايات المتحدة؛ بوصفها البلد صاحب الاتصال الشبكي الأوسع نطاقاً في العالم، هي – أيضاً – البلد الأكثر عرضة للنشاط التخريبي في الفضاء الإلكتروني، سواء أكان ذلك النشاط، في شكل تهديدات للنظام ذاته، أو كان تهديدات موجهة عبر النظام، إلى أهداف موصَّلة شبكياً، وعلى الرغم من مكامن الضعف تلك، فإن إدارة أوباما، ماضية في خطط من شأنها الزيادة – لا التقليص – في اعتماد الولايات المتحدة، على التكنولوجيات الموصَّلة شبكياً؛ لتنفيذ تعاملاتها التجارية، ومراقبة النظم الحسّاسة، والاضطلاع بمسؤوليات الحكم، وتحدِّد "الخطة الوطنية للنطاق العريض"، الوصول الموسَّع للنطاق العريض؛ بوصفه «أساس تحقيق النمو الاقتصادي، وإيجاد الوظائف، وبلوغ التنافسية العالمية، والارتقاء بسبل الحياة»،[9] وتحدد الخطة ستة «أهداف؛ للوصول إلى أمريكا عالية الأداء»، تتيح من خلالها نظم الإنترنت، مكاسب كبيرة جديدة، على صعيد الكفاءة، في كل قطاع من القطاعات الاقتصادية، وفي الحياة اليومية لكل مواطن أمريكي، من دون استثناء، وتشمل الأهداف: إرساء شبكة وطنية للنطاق الواسع للمستجيبين الأوائل **first responders**؛ لتوفير الاتصال المتبادل في أوقات الكوارث، وشبكة "ذكية"، تصل أفراد المستهلكين بشبكة الكهرباء؛ لرصد استخدام الطاقة، ومعدله في الزمن الحقيقي؛ وبالنظر إلى بيئة التهديد الإلكتروني الحالية، نجد أن توسيع نطاق اعتماد الولايات المتحدة، ينطوي على سذاجة كبرى، ووضع أسوأ تصبح فيه الولايات المتحدة، عرضة لتهديدات أطراف حكوميين وغير حكوميين، يسعون لتجاوز ساحة المعركة، وإيذاء المجتمع الأمريكي، في الفضاء الإلكتروني.

وعلى الولايات المتحدة – لدى سعيها لتقليص تلك التهديدات – أن تراعي أيضاً، أن الأمن ليس هدفاً في حد ذاته، وإنما هو عامل ميسِّر للتبادلات التجارية، والارتقاء بالكفاءة؛ فالأمن المفرط، من شأنه: تقليص قابلية استخدام الشبكة، وإبطاء الحركة، وإقامة الحواجز، أمام الاستخدامات الجديدة والمستخدمين الجدد، وبينما توجد ضرورة لتقوية الحوكمة، فإن من الضروري كذلك، تكييف تلك الحوكمة، بحيث تعالج مجموعة محددة من الهواجس الأمنية التي ترتبط بالجريمة والحرب، والاقتراحات المقدمة من أطراف؛ كالصين وروسيا وأنظمة سلطوية أخرى؛ لتحسين "أمن المعلومات" – وهو التعبير الذي اختارته لذلك – لا تخصّ في الواقع، تلك الهواجس، وإنما ترتبط برغبة أولئك الأطراف في الحدّ من المعارضة، ومن الوصول إلى

المعلومات التي يُرى فيها تهديد لأنظمتها؛ فالاقتراحات بإدخال سبل تعقُّب لجميع الطرود: [أجزاء المعطيات الرقمية packet]، يمكن بمقتضاها على الفور، تعقُّب كل إجراء، يُتّخذ على الشبكة؛ وصولاً إلى فرد على سبيل المثال، من شأنها: إبطاء حركة الإنترنت، ورفع تكلفتها، من دون جني فائدة تُذكر، على صعيد مكافحة الجريمة، أو الحدّ من الحروب، بيد أن تلك الاقتراحات، ستسهم في تضييق قدرة المستخدم العادي، على الوصول إلى المعلومات، والدخول في الحوارات السياسية، من دون أن يُكشَف اسمه، وستجد الجماعات الإجرامية والأجهزة الاستخبارية والجيوش، سبلاً للالتفاف على تلك الضوابط، بينما سيخضع نشاط المستخدم العادي على الإنترنت، لمراقبة تكاد تكون كاملة،[10] ونظام كهذا، سيكون له تأثير خانق في إمكانية استخدام الشبكة، وسيلحق الضرر بالمصالح الأمريكية الممثلة بالترويج للحرية والديمقراطية حول العالم، وعلى الرغم من أنه لا يوجد الكثير مما يمكن الولايات المتحدة عمله؛ لإقناع لاعبين؛ كالصين وروسيا وأنظمة سلطوية أخرى، بأن في الوصول غير المقيَّد للإنترنت، وما يصاحبه من انفتاح وحرية تعبير، خدمة لمصالحها القومية، فإن المجتمع الدولي سيصيبه الضرر؛ إذا طُوِّرت الإنترنت العالمية، في الاتجاه الذي يجسد قيم تلك المجتمعات.

ولتفادي هذه النتيجة، والمحافظة - في الوقت ذاته - على الإنترنت، وتوسيع نطاقها؛ بوصفها أداةً للتبادل والكفاءة الاقتصاديين، فإن على الولايات المتحدة، أن تعمل ضمن المنظومة الدولية؛ لكبح الأطراف الفاعلين ذوي النيات الخبيثة، ووضع القواعد المضادة لاستهلال الصراعات في الفضاء الإلكتروني، أما البدائل لهذا النهج، فغير جذابة، وهي تشمل: الاضطرار إلى تقليص التوصيل الشبكي للنظم، وتوسيع نطاق الرقابة للأغراض الأمنية، على رغم تكلفته وصعوبته، والحماية الفعلية للبنى الأساسية الحيوية، في الفضاء الإلكتروني من الأجهزة الحكومية، على غرار الاضطلاع بأمن الشركات الجوية، في أعقاب الحادي عشر من أيلول/ سبتمبر، والتوسع في استخدام القدرات الهجومية؛ لوقف الهجمات؛ وإذا امتنعت الولايات المتحدة عن المشاركة، فإن دولاً أخرى، ستشكل مستقبل الإنترنت، ولكنها ستقوّض الشبكة؛ بوصفها آليةً للتبادل الحر للمعلومات وللتخاطب السياسي، ومن الواضح - في ضوء تلك البدائل - أن الحل المفضل، هو المشاركة الدولية؛ لتحسين أمن الفضاء الإلكتروني، وتحديد الحركة فيه.

مبادئ المشاركة

لم تَعُد الولايات المتحدة الأمريكية طرفاً لا غنى عنه، إزاء ما يتعلق بحوكمة الإنترنت، وامتناعها عن المشاركة في منتديات حوكمة الإنترنت، لن يمنع دولاً أخرى، ذات أهداف تتناقض وأهداف الولايات المتحدة، من تشكيل مستقبل الإنترنت، ولن تنال الولايات المتحدة شيئاً، من الظهور بمظهر المصمِّم على استخدام هجمات الشبكات الحاسوبية من دون قيود، وفي الوقت الذي يتعين فيه على الولايات المتحدة، أن تركز معظم جهودها، على بناء توافق آراء غير رسمي، واستحداث الآليات الدولية للتعاون، فإنها تكون بحاجة إلى أن تشارك؛ وفق شروطها هي، بدلاً من السعي لمنع المناقشة الدولية للموضوع؛ والحديث لن يعود عليها بخسارة تُذكر.

وعلى الولايات المتحدة - من حيث المبدأ العام - أن تدعم العمليات التي تسمح لممثلين من المجتمع التقني، والقطاع الخاص، وأوساط المستخدمين والمستهلكين، أن يشكِّلوا السياسات، وتفادي العمليات التي تكون الدولة مركزها؛ لمعالجة المسائل التقنية، بيد أن المنظمات الحكومية الدولية ضرورية؛ لخضوع الإنترنت لسيادة القانون، ومن خلال المشاركة، تستطيع الولايات المتحدة أن تضع الحلول للتحديات الأمنية، في الفضاء الإلكتروني، على نحو يتفق والمصالح الأخرى المتأتية من اتساع نطاق التجارة الدولية، وتحقيق المزيد من الكفاءة الاقتصادية، وسيتعين على الولايات المتحدة، أن تضع أجندات منفصلة، واستراتيجيات؛ لتحقيق تلك الأجندات، في مجالات الجريمة، والحدّ من دور الدول، واستحداث المعايير الآمنة، ولكنْ، ثمة مجموعة من المبادئ الشاملة التي ينبغي أن توجِّه المشاركة الأمريكية عموماً، في هذا المجال.

اعتماد "نهج شبكي وموزَّع"

على الولايات المتحدة - لدى سعيها لتحقيق مصالحها الوطنية في الفضاء الإلكتروني - أن تدعم العمليات المفتوحة التي ترحِّب بطائفة واسعة من المشاركين، من: الوسط التقني، والقطاع الخاص، وجماعات المستخدمين والمستهلكين؛

لتشكيل السياسات، وتجنُّب العمليات التي تكون الدول مركزها؛ لمعالجة المسائل التقنية؛ ذلك أنه ما من منتدى، يمكنه - وحده - أن يشمل جميع القضايا واللاعبين المعنيين بتبديد الهواجس الأمنية، في الفضاء الإلكتروني، وعلى الولايات المتحدة - بدلاً من ذلك - أن ترعى طائفة من المنتديات - بعضها متعدد الأطراف، وبعضها ثنائي، وبعضها إقليمي - للتصدي لتلك التحديات، وقد يلزم إنشاء ائتلافات منفصلة؛ لمعالجة الأجندة التقنية، والجوانب المختلفة من الأجندة القانونية الدولية؛ ومن ذلك: الجريمة، وتجسس الشركات، والصراعات بين الدول، وتستطيع الائتلافات الإقليمية، أن تثبت فعاليتها أيضاً؛ فعلى الرغم من أن التهديدات الإلكترونية، لا تتباين كثيراً من إقليم إلى آخر، فإن بلوغ سلسلة من الاتفاقات، ضمن المنظمات الإقليمية، قد يكون أسهل من بلوغ اتفاق عالمي، وبدلاً من السعي لاستمالة المستعمرات القديمة؛ للدخول في معاهدات، وضعتها قوى استعمارية سابقة، فإن اعتماد محاكاة اتفاقية مجلس أوربا الخاصة بالجرائم الإلكترونية، في إطار منظمة الدول الأمريكية، والاتحاد الإفريقي، ورابطة أمم جنوب شرق آسيا (آسيان)، قد يكون أكثر تأثيراً، أما الائتلافات العالمية التي تعنى بأنماط مشكلات أكثر تحديداً، فهي - أيضاً - يمكنها أن تكون ذات تأثير؛ فبدايةً، يجب أن تكون تلك الائتلافات مرنة، وغير رسمية، وأن تسعى للحصول على دعم الدول التي تتفق مصالحها ومصالح الولايات المتحدة، أما حلفاء الولايات المتحدة التقليديون، فهم نقطة بداية حسنة، ولكنْ، لا بد من بذل الجهود؛ لاستقطاب ما يزيد على الحفنة التقليدية، من المشتبه بهم من الغربيين، ويمكن أن تشمل قائمة الدول التي سيُطلب دعمها: الدول الإحدى والثلاثين الأعضاء في منظمة التعاون الاقتصادي والتنمية، إلى جانب دول صغرى ودول ذات نمو أقل، وتسعى لمعالجة الجريمة الإلكترونية؛ ومنها: أستونيا والفلبين والجمهورية الدومينيكية.

مساءلة الدول على أفعالها

ظلّ خبراء الاستراتيجية الأمنية، مقيَّدي الحركة؛ بسبب "مشكلة الإسناد، [أو العزو]"، طوال أكثر من عقد، وإسناد الهجمات الإلكترونية؛ [أي تحديد الجهة المسؤولة عنها]، أمر تصعِّبه عوامل أربعة: العامل الأول هو أن الهجمات الإلكترونية، لا تتطلب

قرباً جغرافياً، والثاني هو أنه لا يوجد معادل لنظم الرادار؛ لكشف مصدر الهجوم؛ كما كانت عليه الحال بالنسبة إلى صواريخ الحرب الباردة، والثالث هو أن البروتوكولات التي تحكم حركة الإنترنت، تفتقر إلى الأمن أساساً، ومصدر الطرود يمكن حجبه، والرابع هو أن منفِّذي الهجمات الإلكترونية، يستخدمون - عادةً - نظاماً أو أكثر، من النظم المتضررة؛ بوصفها نقطةَ انطلاق لهجومهم، ويتخطّون الكثير من الحدود الدولية؛ لتعقيد عملية التحرّي.

وبينما توجد ضرورة للسعي لحلّ مشكلة الإسناد، والمشكلات الأمنية الأخرى المرتبطة ببنية الإنترنت، فإن من الضروري، عدم تضخيم مشكلة الإسناد؛ ففي المرحلة الحالية، تُحصر القدرة على شنّ أي شيء يرتقي إلى مستوى "الحرب"، في الفضاء الإلكتروني، في عشرين جماعة على الأكثر، على المستوى العالمي: نصفها من الجهات الحكومية، بينما النصف الآخر جماعات إجرامية خاصة، وهي وثيقة الصلة بدول، وفي حال حدوث هجوم كبير الحجم، فإن قائمة المشتبه بهم، ستكون قصيرة، ومازال السبل التقنية؛ للتعرف إلى منفِّذي الهجمات تشهد تحسناً، ولكنْ، لا بد من عدم إغفال أهمية الاستخبارات والتحقيقات، في العالم الحقيقي، وربما لا يتاح الإسناد اليقيني بالوسائل التقنية على الإطلاق؛ نظراً إلى أن المجرمين والمحاربين الإلكترونيين، سيعملون على استبانة مواضع الضعف، في أي نوع من البروتوكولات، أو نظم مراقبة جديدة، وإن أمكن - على الدوام تقريباً - التوصل إلى ما يشبه السبب المحتمل؛ لإجراء المزيد من التحقيقات.

وعندما تحدث الهجمات الإلكترونية، سوف نجد - في الكثير من الحالات - نفي الدول مسؤوليتها، وإشارة إلى "متسللين، [أو قراصنة] وطنيين"، لا يمكن التعرف إلى هويتهم، أو السيطرة عليهم؛ بوصفهم الجناة المحتملين، كما ترفض الدول، السماح للمحققين، بالوصول إلى المشتبه بهم المحتملين، أو إلى النظم المرتبطة بالحدث؛ لأن ذلك من شأنه: الإخلال بالسيادة الوطنية، وفي مناسبتين على الأقل - ونقصد: مسألة الهجومين على أستونيا وجورجيا - كان ذلك هو الرد الروسي، وبصورة مماثلة، تنفي الحكومة الصينية أي مسؤولية عن الهجمات الإلكترونية التي تنشأ من "أنظمة" كائنة في أراضيها،

وفي أوائل عام 2010، تمكنت شركة جوجل، من تعقّب حملة تسلُّل ناجحة، تم خلالها سرقة معلومات مملوكة؛ [أي سرقة أسرار تجارية]، من جوجل، وشركات أمريكية، بلغ عددها: ثلاثين شركة؛ وصولاً إلى خادمات servers، في الصين، وقد جادل مسؤولون في الحكومة الصينية بأن النظم المستخدمة في الهجمات، هي نظم وكيلة، تم النيل منها؛ بسبب اتساع نطاق استخدام البرامج المقرصنة، والنظم غير الآمنة في بلدهم، وقد يكون هذان التفسيران صحيحين، ولكنْ، في كلا المثالين، وفي ظل وجود أدلّة تشير إلى نشاط إجرامي؛ يستهدف بلداً، ويمكن تعقُّبه؛ وصولاً إلى بلد آخر، فإن عبء الإثبات، يجب أن ينتقل الآن إلى البلد الذي يستضيف النشاط غير المشروع، وعلى الدول التي لا تتعاون في التحقيقات الجنائية، أن تفهم أن عدم التعاون، سيُفسّر على أنه علامة على التواطؤ، ويمكن أن تُحاسَب الدول على أفعالها، وعلى أفعال مواطنيها، وعلى النظم في الفضاء الإلكتروني،[11] وتتطلب الولايات المتحدة، طائفة من الخيارات والآليات؛ لمعاقبة الدول التي تهاجم دولاً أخرى في الفضاء الإلكتروني، بصفة دورية، أو تسمح بأن تُستخدم أراضيها أو نظمها من جماعات إجرامية، وأما الاستجابات فيمكنها أن تشمل الأسلوب التقليدي، وهو الممثل بالاحتجاجات الدبلوماسية، والعقوبات، والعمل العسكري، و - كذلك - التدابير الشبكية؛ ومنها: الارتقاء بمستوى مراقبة حركة الإنترنت الخارجة من الدول غير المتعاونة، وانتهاءً بمنع الدول التي تواصل التغريد خارج السرب، من الوصول إلى شبكات الولايات المتحدة وحلفائها.

القيادة بالقدوة

لا تستطيع الولايات المتحدة أن تدعو الآخرين إلى التحرك، من دون أن تلتزم أيضاً، بضبط النفس، في استخدام القوة في الفضاء الإلكتروني، وكبح مرتكبي الجرائم الإلكترونية في الداخل، واتخاذ الخطوات اللازمة؛ للحد من النشاط الخبيث، في الشبكات الأمريكية، ويجب أن تُبرِز الجهود الدبلوماسية الأمريكية - بوضوح - أن النشاط العسكري والنشاط الاستخباري الأمريكيين، في الفضاء الإلكتروني، إنما يركزان على الدفاع عن الولايات المتحدة، وحماية حرية تدفق المعلومات على المستوى الدولي، وعلى الولايات المتحدة أن تتشدد في التزام ملاحقة أي مواطن، يضلع في "القرصنة الإلكترونية لدوافع سياسية"، ضد

دول أجنبية، وأن تطالب الدول الأخرى، بالقيام بالشيء ذاته، وإزاء ما يتعلق بالجرائم الإلكترونية، لا بد من توفير الأموال لمكتب التحقيقات الاتحادي؛ كي يخصِّص موارد؛ للتحقيق في النشاط الإجرامي الإلكتروني المنطلق من الأراضي الأمريكية؛ ولكنه يستهدف ضحايا في الخارج، وعلى الولايات المتحدة، أن تقود – أيضاً – الجهود؛ لتنظيف حيِّزها من الفضاء الإلكتروني، من خلال: تقليص حصتها من الحواسيب الموصَّلة بالشبكة التي تكون: إما أجزاء من "بوتنتات" botnets – أي شبكات من الحواسيب المصابة التي تُستخدم لشنِّ الهجمات – أو تكون نقاطاً لاستهلال الهجمات، كما أن على الولايات المتحدة، أن تعمل – كذلك – على إرساء آليات؛ لإحباط الهجمات على النظم الأجنبية، المنطلقة من النظم الأمريكية، في الوقت الحقيقي.

السعي للمشاركة الدولية

على الولايات المتحدة أن تسعى؛ مسترشدة بمجموعة من المبادئ، لتحقيق مصالحها على مسارات ثلاثة؛ وهي: أولاً، أن تقود عملية إنشاء مجموعة من نظم دولية أقوى؛ لمكافحة الجريمة في الفضاء الإلكتروني؛ ومادامت المعالجة المنفردة للجريمة الإلكترونية - ثانياً - لن تفضي إلى تقليص التهديدات للشبكة، ولنظامها، بالمستوى الذي يكفي؛ كي تصبح الثقة بها ممكنة، فإن على الولايات المتحدة، أن تنتهج - كذلك - مساراً آخر؛ لتقييد الأطراف الحكوميين في الفضاء الإلكتروني، وأخيراً، على الولايات المتحدة، بذل الجهود؛ لتأمين التكنولوجيات الأساسية للإنترنت.

الحدّ من تهديد الجريمة الإلكترونية

أصبحت الجريمة الإلكترونية، مهنة المجرمين الأذكياء المفضلة؛ نظراً إلى أنها تنطوي على مخاطر محدودة، ومردود عالٍ، وبينما السلطة الوطنية المشروعة، تقيدها الحدود، فإن شبكة الإنترنت ليست كذلك، ويستغل المجرمون هذه الحقيقة، بارتكاب الجريمة الإلكترونية في أحد البلدان؛ انطلاقاً من الحدود الآمنة لبلد آخر، يُفضل أن يتسم بضعف قوانينه، ومحدودية قدراته على إنفاذ القوانين، أو إجراء التحقيقات، أو ملاحقة الجناة؛ ومن هنا، فإن مكافحة الجريمة الإلكترونية، تقتضي أن تسنّ الدول أي قوانين، تعاقب على الجريمة الإلكترونية الدولية، وترسي آليات؛ لوقف الهجمات الناشئة، في أحد البلدان؛ لاستهداف ضحايا في بلد آخر، والتحقيق في تلك الهجمات، وملاحقة مرتكبيها، وتوجد حاجة إلى أن تلقي الولايات المتحدة ثقلها، وراء المبادرات المتعددة الأطراف التي تساعد الدول على تطوير أطرها القانونية، وتعزيز قدراتها، وإرساء آلية لتقويم مدى فعالية الجهود الوطنية؛ لمكافحة الجريمة الإلكترونية، وتنفيذ عملية، تشتمل على حوافز إيجابية وسلبية: [أي عقوبات] تروِّج للتقيد بالمعايير القانونية الدولية.

تركيز الجهود خارج نطاق اتفاقية مجلس أوربا حول الجريمة الإلكترونية

رُكِّزت الجهود الرامية إلى بلورة حلٍ لمشكلة الجريمة الإلكترونية الدولية، في اتفاقية مجلس أوربا حول الجريمة الإلكترونية، وقد صيغت الاتفاقية؛ لتحديد مجموعة أساسية من القوانين التي يتعين على الأطراف في الاتفاقية اعتمادها؛ لتجريم جرائم الحاسوب، وتوفير آلية للتعاون العابر للحدود،[12] وألقت الولايات المتحدة ثقلها، خلف اتفاقية عام 2000، بعد أن تعثرت محاولة محاكمة منشئ الفيروس الحاسوبي المعروف باسم "آي لاف يو" ILOVEYOU؛ ففي تلك الحادثة، تمكنت سلطات تنفيذ القانون، في الولايات المتحدة، من تعقُّب منشئي الفيروس، وهم مجموعة من الطلاب في الفلبين، ولكنها لم تفلح في إقناع السلطات الفلبينية، بتسليم منشئ الفيروس؛ نظراً إلى أن الجريمة التي ارتكبها غير مخالفة لقانون الفلبين، وقد وُضعت الاتفاقية في شكلها النهائي، في تشرين الثاني/ نوفمبر عام 2001، ودخلت حيز التنفيذ في تموز/ يوليو عام 2004، بعد أن صدّقتها دول خمس، وفي أيار/ مايو عام 2010، كان قد صدقها تسعة وعشرون بلداً، بينما كان ينظر في عملية التصديق، سبعة عشر بلداً.[13]

وبينما ساعدت الاتفاقية، على إرساء معيار دولي؛ لتجريم الجريمة الإلكترونية، فإنها لم تؤدِّ إلى تراجع ملحوظ في معدلات تلك الجريمة؛ ذلك أن آليات التعاون الدولي التي استحدثتها الاتفاقية، ثنائية، وتتعلق بالملاحقة القضائية، ولا تفسح المجال؛ لتنسيق نشاطات تنفيذ القانون، عبر الحدود، أو لقيام المهنيين في مجال أمن الشبكة، بتنسيق الحلول التقنية لدى وقوع الهجمات، ويضمّ أعضاء الاتفاقية، بعض أسوأ ملاذات مرتكبي الجرائم الإلكترونية في أوربا الشرقية؛ مثل: رومانيا وبلغاريا، وهناك الكثير من الدول – وخاصة اليابان – لم تكن راغبة في تصديق المعاهدة؛ لأنها اشتُرعت في إطار مجلس أوربا فحسب، وقد أسهمت الاتفاقية في إرساء الإطار القانوني؛ لمواءمة القوانين الوطنية بشأن الجريمة الإلكترونية، وتقديم المساعدة المتبادلة عبر الحدود، بيد أن زيادة عدد الأطراف الموقِّعين على هذه الوثيقة، بصورة خاصة، ليست ضرورية ولا كافية؛ للحد من نشاط الجريمة الإلكترونية العابرة للحدود؛ وخلافاً لمعاهدات الحدّ من التسلح؛ حيث لا يمكن أن تقوم دولة بتخفيض قواتها، إلا بعد اتفاق الأطراف كافة، على تخفيض

للقوات، فإن اعتماد القوانين المتعلقة بالجريمة الإلكترونية، يصبّ في مصلحة دول منفردة، بصرف النظر عن احتمال كون الدول الأخرى، قد اعتمدت تلك القوانين، أوْ لا؛ لأن مجرمي الإنترنت، يميلون إلى عدم قصر نشاطاتهم، على الأهداف الأجنبية.

استخدام فرقة العمل المعنية بالعمل المالي نموذجاً

على الرغم من أن على الولايات المتحدة، أن تدعم، عامةً، العمليات البعيدة عن المركزية، والجامعة للمجتمع التقني، والقطاع الخاص، وجماعات المستخدمين والمستهلكين، فإن هناك مشكلات، لا يمكن معالجتها إلا من خلال الدول، والجريمة الإلكترونية إحدى تلك المشكلات، ولدى استحداث نظام جديد؛ للحدّ من الجريمة الإلكترونية على المستوى الدولي، فإن الهدف يجب أن يكمن في أن تتم معالجة المشكلات القائمة على صعيد التحقيق مع مرتكبي الجرائم الإلكترونية وتوقيفهم وملاحقتهم قضائياً، على نطاق ضيق، وبأقل قدر ممكن من التنظيم، وفي المجالات التي تكون الحكومات وحدها، هي من يقوم بمعالجة مشكلات الفضاء الإلكتروني، فإن عليها أن تقوم بذلك، في أضيق الحدود الممكنة.

كما أن على الولايات المتحدة، أن تروِّج اعتماد القوانين الجنائية، على المستوى الوطني، واستحداث آليات ذات طابع رسمي أخفّ، إزاء ما يتعلق بالتحقيق، والملاحقة القانونية عبر الحدود، من خلال إنشاء جهاز حكومي دولي جديد، يتم تصميمه؛ وفق فرقة العمل المعنية بالعمل المالي، وهي منظمة، أنشئت للترويج لوضع السياسات، وتطوير القدرات الوطنية والدولية؛ لمكافحة تمويل الإرهاب وغسل الأموال،[14] وقد استهلت فرقة العمل – وهي التي أسستها عام 1989، مجموعة البلدان السبعة، بالتنسيق والمفوضية الأوربية، وثمانية بلدان أخرى – عملها، بوضع مجموعة من أربعين سياسة، توصي الدول باعتمادها؛ وسرعان ما اتسع نطاق فرقة العمل، بحيث أصبحت الآن، تضمّ أربعاً وثلاثين دولة، تمثل مجتمعةً معظم المعاملات المالية العالمية، وفي أعقاب الهجمات الإرهابية في الحادي عشر من أيلول/ سبتمبر عام 2001، أضيفت مهمة مكافحة تمويل الإرهاب، إلى مهمات فرقة العمل، وروجعت معاييرها؛ لمعالجة المسألة الجديدة، وإلى

جانب وضع السياسات والمعايير الموصى بها، فإن فرقة العمل، ترصد مدى امتثال الأعضاء لتلك المعايير، وتساعد على تنفيذها، وتتم عملية الرصد؛ على أساس استعراض أقران متعددي الأطراف، في إطار برنامج، يُعرف باسم "التقويم المتبادل"، كما تمخضت فرقة العمل، عن سلسلة من الأجهزة الإقليمية، على الطراز نفسه، تضطلع بمهمات مماثلة، ضمن مناطق جغرافية محددة،[15] ولدى فرقة العمل، طائفة متفق عليها، من المعايير والآليات المحددة؛ لرصد الامتثال، وهي تشكل الأساس الذي تستطيع الولايات المتحدة، ودول أخرى، أن تستند إليه، في تهديد الدول غير الممتثلة، بالحرمان من سبل الدخول إلى الشبكات المالية الدولية.

ولا بد من إنشاء منظمة شبيهة، تقوم، إزاء ما يتعلق بالجريمة الإلكترونية، بما تقوم به فرقة العمل المعنية بالعمل المالي، على صعيد غسل الأموال، وعلى الولايات المتحدة أن تنشئ هذه المنظمة، بالتعاون بينها وبين الدول الأخرى الأعضاء في منظمة التعاون الاقتصادي والتنمية، والدول الأصغر حجماً المؤيدة لجدول أعمال المنظمة، وأن تضع معايير تقويم طلبات العضوية التي تتقدم بها الدول الأخرى، ولا بد أن تبدأ المنظمة، بوضع سياسات نموذجية، تستند إلى اتفاقية مجلس أوربا، ومجموعة أدوات الاتحاد الدولي للاتصالات، بشأن تشريعات الجريمة الإلكترونية، وممارسات مثلى أخرى معترف بها؛[16] وكما هي الحال بالنسبة إلى فرقة العمل المعنية بالعمل المالي، لا بد أن يكتمل العمل، خلال العام الأول من إنشاء المنظمة؛ وإثر وضع السياسات الموصى بها، يجب أن تشرع المنظمة، في تقويم البلدان الأعضاء، من حيث المعايير الموضوعة، كما ينبغي أن توفِّر عمليات التقويم، خطة لتصحيح أي مشكلات يتم التعرف إليها، وأن ترسي عملية للاستعراض الدوري، إزاء التقدم المحرز في معالجة تلك المشكلات.

تسمية ملاذات مرتكبي الجريمة الإلكترونية وفضحها ومعاقبتها

على المنظمة كذلك، أن تجري استعراضاً عالمياً سنوياً، للدول الأعضاء وغير الأعضاء معاً؛ لتقويم الأطر القانونية والقدرات، على تنفيذ القانون والمستويات الشاملة للجريمة الإلكترونية لدى الدول، وأما ما يخصّ المشكلات عبر الوطنية الأخرى، فإن إعداد مؤشر

أو تقرير سنويين، بشأن البلدان الأفضل والأسوأ؛ انطلاقاً من قياسات موضوعية، دعا دولاً كثيرة إلى تحسين سلوكها، وتشمل النماذج، مؤشر الفساد الذي تعدّه منظمة الشفافية الدولية، والتقرير العالمي، حول المخدرات، وهو الذي يعدّه مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ومؤشر شؤون الحوكمة، وهو الذي يعدّه البنك الدولي، وقد شرع منتدى رسم خرائط الجريمة الإلكترونية وقياسها، وهو التابع لمعهد أوكسفورد للإنترنت، في استكشاف القياسات الممكن استخدامها، في مثل ذلك التصنيف،[17] وتلك التصنيفات، ستكون آلية فعّالة؛ لـ "التسمية والفضح" للدول؛ حتى تتصدى لنشاطات الجريمة الإلكترونية، وتنضم إلى عضوية المنظمة الجديدة.

ويمكن – عندئذٍ – استخدام تلك التصنيفات المستقلة؛ أساساً تعمل المنظمة وفقه، مع البلدان الأسوأ؛ لوضع خطط سدّ الفجوات في آلياتها الخاصة بالشؤون القانونية وتنفيذ القانون؛ وفي نهاية المطاف – كما هي الحال بالنسبة إلى توصيات فرقة العمل المعنية بالعمل المالي وتقويماتها – يمكن أن توفِّر تلك العملية، الأساس الذي يتم الاستناد إليه، في معاقبة الدول؛ لعدم تصديها لنشاط الجريمة الإلكترونية، ويمكن فرض العقوبات؛ على أساس ثنائي أو أساس متعدد الأطراف، ويمكنها أن تشمل منع المعونات المالية الإنمائية الهادفة إلى تطوير البنى الأساسية للإنترنت، أما الدول التي لا تنظِّف حركة المرور الدولية للإنترنت لديها، فيمكنها أن تخضع لـ "فحص المحتوى العميق"،* أو مستويات مرتفعة أخرى من المراقبة؛ بما يبطئ تدفق حركة المرور [لديها]، كما أن عدم تحقيق تحسّن، يمكن أن يؤدي – بوصفه ملاذاً أخيراً – إلى أن تقوم الدول الأعضاء في المنظمة، بوضع طوائف من بروتوكولات الإنترنت الوطنية الخاصة بالدول الأكثر انتهاكاً على القائمة السوداء.[18]

ربط مساعدات تطوير البنى الأساسية للإنترنت بالتعاون في مجال الجريمة الإلكترونية

على المنظمة الجديدة أن تعمل أيضاً، مع المنظمات الدولية التي تروِّج لتطوير البنى الأساسية للإنترنت؛ لضمان أن تنفَّذ تلك الاستثمارات، مقترنةً بالاستثمارات في تطوير القدرات، إزاء ما يتعلق بالجوانب القانونية والتصدي للحوادث وإنفاذ القانون، وهذا

* أو عملية التحليل العميق للحُزَم؛ أي قيام مزود خدمة الإنترنت، بتتبع البيانات التي تمر عبر الشبكة. (المترجم)

الجهد يمكن الترويج له داخل الحكومة الأمريكية أيضاً؛ فالمشروعات التي تضطلع بها وكالة التنمية الدولية التابعة للولايات المتحدة؛ لمدّ شبكات كابلات الألياف البصرية في البلدان النامية، يجب أن تتم بالتنسيق بينها وبين المساعدة القانونية المقدمة من وزارة العدل؛ لتطوير القدرات في مجال التحقيقات والملاحقة القضائية، وفي الوقت الحالي، لا يوجد رابط بين الجهدين، وعلى وزارة الخارجية الأمريكية، أن تضغط على الدول الحليفة والمنظمات الإنمائية الدولية؛ لاعتماد سياسات مماثلة.

إنشاء مراكز عمليات لتنسيق طلبات المساعدة

يمكن أن تساعد المنظمة، أخيراً، على حلّ مشكلة التنسيق الدولي؛ لوقف الجرائم الإلكترونية المستمرة، والتحقيق في الهجمات التي تعبر الحدود الدولية، إثر وقوعها وملاحقة مرتكبيها، والعملية الثنائية الحالية بطيئة ومضنية وعالية التكلفة، حتى بالنسبة إلى الولايات المتحدة، بسفاراتها التي لا ينقصها الموظفون وملحقاتها القانونية، وهي المنتشرة في مختلف أنحاء العالم، فضلاً عن الدول الصغيرة التي كثيراً ما تقع ضحية للجريمة الإلكترونية، وقد وضعت المجموعة الفرعية حول جرائم التقنية العالية التابعة لمجموعة البلدان الثمانية، أسس ذلك الجهد، من خلال إرساء آلية للتعاون، بشأن الجريمة الإلكترونية، تعمل على مدار الساعة طوال أيام الأسبوع، وهذا الجهد يمكن تحسينه من خلال جعل المنظمة تنشئ مراكز عمليات في جميع أنحاء العالم، يعمل فيها موظفون في مجال تنفيذ القانون من الدول الأعضاء، ويمكن تلك المراكز أن توفِّر موارد متاحة بصورة مستمرة، ورابطاً قيّماً بين موظفي تنفيذ القانون، ومراكز عمليات أمن الشبكة، وينبغي أن يكون من بين أهداف ذلك الجهد، استحداث آلية، يتم من خلالها، إرسال الطلبات التي ترد من الوكالات الحكومية والقطاع الخاص، في إحدى الدول، إلى السلطات في دولة أخرى؛ ومن ثمّ تمريرها إلى مشغّلي الشبكة؛ لإغلاق مزوِّدي خدمة القيادة والتحكم، أو مضيفي البوتنتات.

الحدّ من العمل الحكومي في الجريمة الإلكترونية

إن الجريمة الإلكترونية، ما هي إلا جزء من النقص الأمني الحالي في الفضاء الإلكتروني، وقد يكون في النشاط الحكومي، تقويض للثقة في الشبكة، أكثر مما يكون في

نشاط مرتكبي الجريمة الإلكترونية، وبينما يمكن التهوين من الجريمة الإلكترونية؛ بوصفها تكلفة للقيام بالأعمال، فإن أعمال الأطراف الحكوميين، تهدد نموذج الموصولية ذاته، وما يتبعه من مكاسب، على صعيد الكفاءة؛ ولأن الأطراف الحكوميين لديهم قدرات عالية عموماً، فإنه ما من شيء موصول بالشبكة، يعد بعيداً عن متناول يدهم؛ ولذا، فلا بد من كبحها بوسائل أخرى؛ إذا صعب كبح الدول بواسطة الدفاعات التقنية، وإذا لم يمكن فرض القيود، فقد تؤدي مكاسب الكفاءة المتأتية من الاتصال بالشبكة، إلى تحمّل تكلفة تفُوق قيمتها، وإذا تواصل الاستغلال الروتيني للبنى الأساسية الحساسة، فإن إعداد ميدان المعركة ذاته، قد يؤدي إلى نشوب صراعات لم تكن لتنشب، وإذا استمرت الدول في استهداف الملكية الفكرية للشركات الأجنبية، ونقل تلك الملكية إلى الشركات الوطنية، فإن ذلك قد يؤدي إلى تفكُّك النظام العالمي للبحث والتطوير، وهو الذي يتيح تنفيذ العمل على مدار الساعة.

إنهاء الاعتراض على المحادثات بشأن الحرب والتجسس في الفضاء الإلكتروني

لمعالجة تلك الهواجس، على الولايات المتحدة أن تعمل على وضع قواعد جديدة لسلوك الدول في الفضاء الإلكتروني؛ فطوال العقد الفائت، كانت الولايات المتحدة تتخذ موقفاً معارضاً لأي مناقشات حول هذه المجالات، وكانت تسعى لحصر تركيز المجتمع الدولي على معالجة الجريمة الإلكترونية، والاعتراض الأمريكي نابع من رؤية؛ مفادها: أن الدول لن تحترم التزاماتها بتقييد نشاطاتها في الفضاء الإلكتروني، وأن التحقق من وفاء الدول بالتزاماتها، سيكون أمراً شبه مستحيل،[19] بيد أن هذا الموقف نابع من تطبيق تجربة الحدّ من التسلح إبّان الحرب الباردة، وهو أمر لا يسهل تطبيقه على مشكلة أمن الفضاء الإلكتروني الحالية؛ فالاتفاقات الدولية المحدودة والمركزة، يمكنها أن تفيد الولايات المتحدة في بعض الحالات، وعلاوة على ذلك، فإن عدم رغبة الولايات المتحدة، في خوض مفاوضات حول هذا الموضوع، يزيد مصداقية الرأي الذي مفاده: أن الولايات المتحدة تسعى للسيطرة على الفضاء الإلكتروني.

والولايات المتحدة هي شبح الفضاء الإلكتروني الأكثر إثارة للخوف؛ بالنظر إلى دورها التاريخي في تطوير التكنولوجيات الأساسية، وارتفاع مستوى القدرات، ضمن: الجيش الأمريكي، وأجهزة الاستخبارات الأمريكية، أما المحافظة على تفوق القدرات الأمريكية – من حيث الاستغلال والهجوم مقارنة إلى المنافسين كافة – فأمر يخدم المصالح الأمريكية حقاً! ولكن، من المؤكد أن ما لا يخدم تلك المصالح، هو إدراك الآخرين أن الولايات المتحدة، تمتلك تلك القدرات وتستغلها، وأما عسكرة الفضاء الإلكتروني، فتشكل تهديداً على وحدة الشبكة وعالميتها وتبادليتها، وهذه العوامل كان لوجودها أثر كبير في: تحقيق النمو الاقتصادي الواسع النطاق، وتوثيق العلاقات بين الدول، من خلال التجارة المشتركة، وتسريع تبادل الأفكار عبر الحدود الثقافية والدولية، ولا يؤدي رفض المشاركة العلنية في مفاوضات حول الحدّ من الحرب الإلكترونية، إلا إلى زيادة المخاوف، بشأن كون الولايات المتحدة تسعى للسيطرة على الفضاء الإلكتروني، وتخطط لاستغلال النطاق؛ لنيل ميزات قتالية، وعلى الولايات المتحدة، أن تبذل ما في وسعها لمواجهة ذلك التصور، وبينما نجد أن المفاوضات ربما لا تفضي إلى إبرام اتفاقية، فإنها لن تسبب أيضاً، أي أضرار، وقد تبنَّت إدارة أوباما مبدأ الحوار على المستوى الدولي، ولا يجوز أن تُستثنى الحرب الإلكترونية من ذلك، وتعدّ مشاركة الولايات المتحدة في فريق الخبراء الحكوميين، وهو التابع للأمم المتحدة، بداية طيبة، ولكن التواصل يجب أن يكون أوسع وأعمق بكثير.

بيد أن التواصل لا يعني أن الولايات المتحدة مضطرة إلى قبول خيارات الاتفاقيات القائمة التي لا تصب في مصلحة الولايات المتحدة؛ فالاقتراح الروسي الحالي بشأن الحدّ من التسلح في الفضاء الإلكتروني، يُلزم الأطراف الموقِّعين بالامتناع عن تطوير قدرات إلكترونية هجومية، أو الضلوع في التجسس الإلكتروني، بينما يخلو من الآليات الناجعة للتحقُّق، وسجل اتفاقيات الأسلحة الكيميائية والبيولوجية، يثير الشكوك في شأن أن بالإمكان أن تفضي الالتزامات التي لا مجال للتحقق منها، إلى تقليص حقيقي، وعلاوة على ذلك، نجد – حال وفاء الولايات المتحدة بالتزاماتها، وتخلُّف الدول الموقِّعة الأخرى – أن اتفاقية من دون آلية تحقُّق؛ تعني أن الولايات المتحدة ستخسر ميزاتٍ استراتيجية.

والتركيز على تقييد تطوير الأسلحة الإلكترونية، ينمّ عن عدم فهم للطبيعة الحقيقة للحرب الإلكترونية؛ فالتهديدات المتقدمة في الفضاء الإلكتروني، لا تكمن في البوتات bots،* أو الديدان worms،** وإنما في العنصر البشري، والسلاح الأقوى ليس القنابل المنطقية،*** أو أحصنة طروادة،**** وإنما البشر الذين يصممونها، ويمكنهم استخدامها؛ بوصفها جزءاً من مجهود مستمر منظم؛ للوصول إلى النظم المستهدفة، واستغلالها؛ سعياً لنيل الميزات المعلوماتية وإفساد البيانات أو تدميرها، وعلاوة على ذلك، فإن أي برنامج دفاعي، يتطلب إتقان العمليات الهجومية؛ حتى يمكن صدّ تلك العمليات، وفي الحرب الإلكترونية، نجد أن القدرة على استنساخ البرامج الحاسوبية؛ تعني - على الفور - أن أي خطوات يتم تطويرها؛ لأغراض اختبار التدابير المضادة، يمكنها أن تتحول بسرعة إلى عملية هجومية، وفي ظل هذه الحقيقة، لن تحقق محاولات الحدّ من تطوير العمليات الإلكترونية الهجومية النجاح؛ لأن التحقق من كون الدول لم تطوِّر مثل تلك القدرات، سيكون أقرب إلى المستحيل.

تفحُّص خيارات الاتفاقيات واستحداث القواعد في مواجهة استهداف النظم المدنية

إن وجود مشكلة التحقق؛ لا يعني أنه لا توجد مسائل، يمكن المفاوضات والاتفاقات الدولية، أن تعالجها على نحو مفيد؛ فبدلاً من التركيز على الحدّ من تطوير الأسلحة الإلكترونية، يجب على جهود الاتفاقيات، أن تركز على الحدّ من اختراق الجهات الحكومية للنظم المدنية، ذات القيمة الاستخبارية المحدودة أو ذات القيمة الاستخبارية المعدومة، وفي المرحلة الراهنة، هناك الكثير من الدول التي تشنّ عمليات إلكترونية هجومية، تحت غطاء منفصل، ولكنه ذو صلة؛ ومفاده: "التجسس"، و"إعداد ميدان المعركة"، وأما الأفعال؛ من قبيل: اختراق شبكات الكهرباء في الدول الأجنبية، بحيث يمكن تعطيلها في زمن الحرب، فتؤدي إلى زعزعة الاستقرار، وزيادة الاحتمالات، بأن

---

* البوتات أو روبوتات الشبكة العنكبوتية: تطبيقات برامجية تقوم بمهمات آلية على الإنترنت؛ ومنها: الهجمات المنسَّقة على الحواسيب الموصولة شبكياً. (المترجم)

** برامج يراد بها تدمير حواسيب متصفحي الإنترنت، أو سرقة بياناتهم. (المترجم)

*** رموز تُزرع عمداً، داخل نظم براجية، وتُطلِق وظائف خبيثة، عندما تتوافر شروط معينة. (المترجم)

**** برامج خبيثة، تبدو وكأنها تؤدي رغبة المستخدم، ولكنها تمهد الطريق؛ كي يصبح حاسوبه مستباحاً للدخول غير المأذون به. (المترجم)

يتسع نطاق الصـراع في الفضاء الإلكتروني إلى العالم المادي، وعـلى الولايـات المتحـدة، أن تسعى أيضاً، لتفادي أن تتحول الهجمات الإلكترونية إلى شكل خطير جديد، مـن أشـكال الاحتجاج؛ أي مرحلة وسطى ما بين بذل المساعي [الدبلوماسية]، والقيام بردٍّ عـسكري، وإذا أصبحت الهجمات الإلكترونية شكلاً مقبولاً من أشكال الاحتجاج الدولي، فـإن آثـار ذلك، قد تسهم بشكل خطير في زعزعة الاستقرار الاقتصادي، ويمكنها أن تفـتح المجـال أمام الصـراعات العسكرية التقليدية.

والاتفاقات الدولية التي تقـتضي منـع اخـتراق شـبكات الكهربـاء، والقطـاع المـالي، والمكونات الأخرى للبنى الأساسية المدنية، قد تـصب في مـصلحة الولايـات المتحـدة، في نهاية المطاف، ولكنْ في المرحلة الحاليـة، نجـد أن الـدول في معظمهـا – ومنهـا الولايـات المتحدة – غالباً ما لا ترغب في التخلي عن القيمة الاستخبارية المستقاة من اسـتغلال تلـك النظم، وعلى حكومة الولايات المتحدة، أن تشرع في عملية لاستبانة في أي ظروف ستخدم أو لا، تلك الاتفاقـات، المـصالح الأمريكيـة: (هـشاشة تلـك الـنظم، والتكلفـة المرتبطـة بحمايتها قد تفوق – في نهاية المطاف – المنافع المتحصَّل عليها من استغلال نظـم الخـصم)، وبينما قد يكون هذا الاقتراح، من السابق لأوانه أن يحظـى بالـدعم الكـافي، مـن الحكومـة الأمريكية والحكومات الأجنبية، فإن ثمة مجالين جاهزين؛ كي يتم التوصل إلى اتفـاق دولي بشأنهما؛ للحد من تدخّل الدولة في الفـضاء الإلكـتروني، وفي كـل مجـال مـنهما، لا توجـد مصالح استخبارية مهددة، وعلى الولايات المتحدة أن تضع اقتراحات للمعالجـة المنفـصلة لمسألتي الأمن والحرمة للعمليات الأساسية التي تتيح عمـل الإنترنـت، ولحظـر هجـمات حجب الخدمة.

الاعتراف بالجذر بوصفه قيمة استراتيجية دولية

كان الجذر root، في صلب حوكمة الإنترنت، منذ اسـتحداث نظـام اسـم النطـاق في ثمانينيات القرن العشرين، والنظام يوفِّر الرابط الضروري بين أسـماء النطـاق التـي يمكـن البشر قراءتها؛ مثل: CFR.org: [اسـم العنـوان الـشبكي لمجلـس العلاقـات الخارجيـة]، وعناوين بروتوكولات الإنترنت التي يمكن الأجهزة قراءتها؛ من قبيـل: 66.40.21.148.

ويعتمد النظام على 13 خادماً رئيسياً؛ لتوفير معلومات موثوق بها، بالنسبة إلى النطاقات من المرتبة العليا؛ (مثل:.com وnet. وus. وjp.،... إلخ)؛ لبدء عملية الاستجابة لطلب يتعلق بخادم صفحة شبكية أو بريد إلكتروني، وهناك جهود تُبذل؛ لتحسين أمن الجذر، لكن عمليات الجذر، ماتزال عرضة لمحاولات الاختراق، ولهجمات حجب الخدمة الموزَّعة، وحجب الخدمة الواسعة النطاق؛ ولأن المعلومات المتضمَّنة في ملف منطقة الجذر، هي – بطبيعتها – مفتوحة للعموم، فما من قيمة استخبارية يمكن جنيها من محاولة الوصول إلى خادم جذري، وأما التوصل إلى اتفاق يُعترف بالجذر؛ بوصفه قيمة استراتيجية دولية، لا يجوز للدول أن تسعى لتعطيلها، فسوف يصب في المصلحة الأمريكية، وقد يكون بمنزلة خطوة أولى، باتجاه الحدّ من التوترات في الفضاء الإلكتروني، وماتزال سيطرة الولايات المتحدة على الجذر، إحدى القضايا التي هي محلّ خلاف، وبينما كانت الرغبة الأمريكية في المحافظة على هذا الدور، نابعة من ضمان استمرار أداء الجذر لوظائفه، فقد يكون من مصلحة الولايات المتحدة، أن توجد آلية دولية، تتولى الإشراف على الجذر؛ بوصفه جزءاً من صفقة كبرى، بشأن حوكمة الإنترنت.

السعي لاتفاقية تحظر هجمات حجب الخدمة

إن التوصل إلى اتفاق لحظر هجمات حجب الخدمة، سيركز – على غرار اتفاق حماية الجذر – على مشكلة ضيقة، لا يعقِّدها جمع الاستخبارات، أما هجمات حجب الخدمة فهي – بطبيعتها – من الأسلحة البدائية التي لا تتطلب اختراق الشبكات، وإنما تعطيلها، وهي أيضاً، سلاح فتّاك، سبق أن استخدم في العمليات الإجرامية، وكذلك في الصراعات التي تنشب على مستوى الدول، وفي ثلاثة أمثلة على الأقل، ضلعت الحكومة والجيش في روسيا في هجمات لحجب الخدمة، أو شجّع كلاهما على ذلك، ضد دول أجنبية؛ فعطَّل هذا البنية الأساسية للإنترنت والخدمات المعتمدة عليها لدى الضحايا؛ ومن بين تلك الهجمات: الهجوم الذي وقع عام 2007، واستهدف أستونيا، وهجوم عام 2008؛ مستهدفاً جورجيا، وهجوم عام 2009، ضد قيرغيزستان، وخلافاً لاستغلال الشبكة الحاسوبية، وهو الذي يمكن استخدامه للتخريب أو التجسس، فإن هجمات

حجب الخدمة، لا يمكنها أن تساعد إلا على تخريب أحد النظم؛ ومن هنا، فإن على الولايات المتحدة، أن تروِّج لاتفاقية من شأنها، إلزام الأطراف الموقِّعين بسياسة، يتم - وفقها - الحدّ من هجمات حجب الخدمة، خارج نطاق الصراعات التقليدية، ومنع تلك الهجمات بمقتضى معاهدة دولية، يمكن أن يكون الخطوة الأولى؛ لتأسيس المسؤولية في الفضاء الإلكتروني؛ ذلك أن هجمات حجب الخدمة في معظمها، ينفِّذها مجرمون؛ لأغراض الابتزاز، والمساعدة التي تقدمها الدول؛ لإحباط هجوم موزَّع لحجب الخدمة، يمكن استخدامها؛ للحكم على كون الدولة قد غضَّت الطرف عن الهجوم، أو أنه وقع ضد رغبتها، وإذا ساعدت الدول على وقف الهجوم، فعندئذٍ يجب التعامل وإياه؛ بوصفه عملاً إجرامياً، وإذا لم تستجب الدول كذلك، فإن ذلك سوف يجب أن يُفهم، على أنه إشارة إلى موافقة رسمية على الهجوم، وأن يعامَل - من ثم - بوصفه عملاً عدائياً.

وضع الأجندة التقنية

ظلَّ تركيز الأوساط التقنية للإنترنت، حتى وقتنا الحاضر، منصباً على التبادلية؛ أي قابلية تبادل المعلومات، ومع استمرار تطوّر التكنولوجيات التي تتيح عمل الإنترنت، فإن هناك حاجة إلى أن يُحوَّل ذلك التركيز نحو الأمن؛ فالتكنولوجيات الأساسية للإنترنت، كانت مصممة لشبكة مغلقة، يخضع فيها الدخول للسيطرة المحكمة، ويحظى جميع المستخدمين بالثقة بهم، ولم تكن تلك التكنولوجيات مستحدَثة، أو مصممة للأغراض التي تُستخدم الآن من أجلها، وهذه المشكلة - وهي التي تدركها الأوساط التقنية منذ زمن - ماتزال بانتظار المعالجة، وقد حددت "الوثيقة الوطنية الأمريكية لتأمين الفضاء الإلكتروني" لعام 2003، مكامن الضعف، ضمن ثلاثة من "بروتوكولات الإنترنت الرئيسية"؛ وهي: بروتوكول الإنترنت، ويُسترشد به في توجيه البيانات من المصدر إلى الوجهة المقصودة عبر الإنترنت، ونظام اسم النطاق، وهو يحوِّل أرقام بروتوكول الإنترنت إلى عناوين شبكية، يمكن التعرف إليها، وبروتوكول البوابة الحدودية، وهو الذي يوفِّر الاتصال بين الشبكات؛ لإيجاد "شبكة الشبكات"،[20] ولا يوجد في أي من تلك البروتوكولات آلية مدمجة؛ للتحقق من الأصل أو صحة المعلومات المرسلة إليها؛ بما

يعرِّضها للاحتيال أو التلاعب، من الأطراف السيِّئي النية، وقد أقرّت استراتيجية عام 2003، تلك المشكلات؛ ولكنها خلصت إلى أن «الصناعة الخاصة، تقود الجهد الذي يضمن تطوّر الوظائف الرئيسية للإنترنت، على نحو آمن»، وقصرت دور الحكومة الاتحادية، على تنسيق «الشراكات القائمة بين القطاعين العام والخاص؛ لتشجيع... اعتماد بروتوكولات أمن محسَّنة»،[21] وبعد مضي نحو عقد، ماتزال الإنترنت تعاني المشكلات ذاتها، وفي هذه المرحلة، يمكن الخلوص - بثقة - إلى أن نموذجي "التنسيق"، و"التشجيع"، لما يؤتيا بعدُ النتائج المرجوة، وهناك حاجة إلى أن تتحلى الحكومة الاتحادية بمستوى قيادة أقوى.

وتستطيع الولايات المتحدة - من خلال التحلّي بالقيادة، وتقديم المساعدة التقنية والتمويل - أن تعزِّز التطوير والاعتماد لمجموعة جديدة من البروتوكولات الآمنة التي ستعالج الكثير من مكامن الضعف في البنية الحالية للإنترنت، وتمنع - في الوقت ذاته - التطوير والاعتماد لبروتوكولات، تفرط في التوجه نحو استحداث دولة مراقبة على الإنترنت، أو نشوء خطر تفكك الإنترنت، إلى سلسلة من الشبكات الوطنية المبلقنة، [نسبة إلى البلقان]، والمنفصلة؛ والهدف - كما كتب ماركوس ساكس - هو تفادي نشوب "حرب باردة تقنية"، تطوِّر خلالها الولايات المتحدة والصين وأوربا: «شبكات حاسوبية مختلفة تقنياً، وغير قابلة للتشغيل المتبادل؛ على أساس بروتوكولات وقواعد، تتناسب وقيم كل مجتمع وأخلاقياته ونظمه القانونية».[22]

توجيه مؤسسة العلوم الوطنية لوضع تحدٍّ تقني أمام فرقة العمل المعنية بهندسة الإنترنت لوضع بروتوكولات آمنة

إن الطريقة المثلى لاستباق هذه النتيجة، هي المساعدة على استحداث مجموعة من البروتوكولات التي تبدِّد الهواجس الأمنية، على الوجه الكافي، من دون تفكيك الإنترنت، أو تحويلها إلى منصة عالمية للسيطرة الحكومية؛ فطوال أكثر من عقدين، قادت فرقة العمل المعنية بهندسة الإنترنت، تطوير المعايير التقنية التي تتيح للإنترنت أن تؤدي وظائفها، والفرقة وأعضاؤها، مجتمع مفتوح من الخبراء التقنيين من مختلف أنحاء العالم، قاد تطوّر

الإنترنت على مدى جيل، ويجب أن يُمنح الفرصة لمعالجة أوجه القصور الأمني التي تحيط بالشبكة الحالية، ويجب على حكومة الولايات المتحدة، أن تضع - بالتنسيق بينها وبين حلفائها - أمام الفرقة، التحدي الممثل باستحداث مجموعة جديدة من البروتوكولات الأكثر أمناً؛ والهدف - وهو الذي كان جون مايكل "مايك" ماكونل، المدير السابق للاستخبارات الوطنية، أبلغ المعبّرين عنه - يجب أن يمثل بـ «إعادة تصميم الإنترنت، بحيث تزداد القدرة على: إدارة الإسناد والموقع الجغرافي وتحليل الاستخبارات وتقويم الأثر - أي [الإجابة على الأسئلة]: من الفاعل؟ ومن أين؟ ولماذا؟ وما النتيجة؟»،[23] ولكنْ لا يجوز لها أن تسعى لأن تدمج في رموز الإنترنت الأساسية، إسناداً تاماً، يكون هو الأداة النهائية لدولة المراقبة.

وعلى مؤسسة العلوم الوطنية، أن تقود الجهد؛ لبلورة التحدي التقني، على أن يتم ذلك بالتنسيق بينها وبين الوكالات الاتحادية المعنية، والقطاع الخاص، والمؤسسات الأكاديمية، ويجب أن تركز المرحلة الأولية، على تحديد المشكلات الناجمة عن انعدام الأمن في الإنترنت، واستبانة: هل من الممكن معالجة تلك المشكلات، من خلال استحداث معايير تقنية جديدة أو لا؟ وكيف يتم ذلك؟ وعلى المؤسسة أن تنتقل - بعد ذلك - إلى طرح التحدي، والإشراف على نظام من المنح المقدمة، عن طريق فرقة العمل المعنية بهندسة الإنترنت، ويجب أن يتضمن التحدي، موعداً نهائياً يحلّ بعد أربع سنوات؛ لتقديم مجموعة من البروتوكولات الآمنة، والشروع في تنفيذها، ويجب أن يوضَّح - لدى تقديم التحدي - أن عدم الالتزام بالموعد النهائي، سينجم عنه استهلال مجهود اتحادي؛ لاستحداث بروتوكولات جديدة، وعلى الولايات المتحدة، أن تموِّل ذلك النشاط، وأن تسعى لنيل دعم دول أخرى، تتفق والنهج؛ كما صيغ، وكما عبِّر عنه؛ لضمان أن يستجاب للتحدي، وأن تتسق البروتوكولات المستحدثة والأهداف الشاملة للولايات المتحدة؛ لتطوير الفضاء الإلكتروني، وبعد ذلك، يجب توفير الحوافز التي ستساعد على تنفيذ تلك الأهداف.

تنظيم الجهد الأمريكي

تعكف القيادة الإلكترونية، على دمج الوحدات الإلكترونية، في: الجيش والبحرية وسلاح الجو والمارينز الأمريكي، ضمن جهد منسق؛ لحماية شبكات وزارة الدفاع، ودعم المهمات البرية والبحرية والجوية، وتنفيذ عمليات هجومية في الفضاء الإلكتروني، عندما تصدر لها الأوامر بذلك، والتشريع الذي ينظر فيه مجلس الشيوخ، سيعهد إلى وزارة الأمن الوطني، مهمة تأمين جميع النظم الحكومية المدنية، ويمنحها صلاحيات إضافية؛ لتنظيم البنى الأساسية الحساسة، في القطاع الخاص، توخياً للأمن الإلكتروني، وهناك ضرورة لجهد موازٍ؛ لضمان أن تكون الجهود الدبلوماسية، مع الدول الأجنبية - ضمن ملتقيات حوكمة الإنترنت - منسَّقة، وحائزة على الموارد اللازمة، وساعية لتحقيق أهداف أمريكية محددة.

تعيين نائب منسق البيت الأبيض للأمن الإلكتروني لحوكمة الإنترنت

في عهد إدارة بيل كلينتون، وُلِّيت موظفة واحدة، وهي آيرا ماجازينر، فعلياً، إدارة وضع سياسة حوكمة الإنترنت، والتواصل ومنتديات حوكمة الإنترنت، وقد اتسع نطاق المسألة كثيراً، بحيث لم يعد يمكن شخصاً واحداً أن يديرها بفعالية وحده، ولكنْ، لا بد أن يضطلع البيت الأبيض، بدور الريادة، إزاء ما يخصّ حوكمة الإنترنت؛ لتنسيق رسم السياسات، والإشراف على تنفيذها، والتشريع الذي من شأنه توسيع نطاق الصلاحيات الممنوحة لوزارة الأمن الوطني، سيكفل كذلك، أن يُنشأ - ضمن المكتب التنفيذي للرئيس - مكتب سياسات الفضاء الإلكتروني؛ على أن يناط به، الدور القائم لمنسق الأمن الإلكتروني، مع تعزيز ما لذلك المنصب، من صلاحية وميزانية وموظفين، ويجب أن يكون لمدير هذا المكتب، نائب لتنسيق السياسات الأمريكية، في مجال حوكمة الإنترنت، إلى جانب موظفين، يتولون الإشراف، بشكل يضمن النهوض بالأجندة الأمريكية، في مجال الفضاء الإلكتروني، في كل فرصة.

إنشاء مكتب جديد للشؤون الإلكترونية في وزارة الخارجية

لا بد من إعادة تنظيم وزارة الخارجية، وتزويدها بالموظفين؛ سعياً لتنفيذ الأجندة الأمريكية، في مجال الفضاء الإلكتروني، بحيث يتم التركيز - أساساً - على تأمين النطاق،

في جميع الملتقيات والعلاقات الثنائية التي تتعلق بالفضاء الإلكتروني، وعلى الرغم من أن وزارة الخارجية، تركز بإفراط في المرحلة الحالية، على مسألة حرية الإنترنت، بشكل يلحق الضرر بالأمن الإلكتروني، فإن ذلك الانحياز، يمكن تصحيحه، من خلال تكليف الوزارة بمهمة واضحة، إزاء ما يتعلق بحوكمة الإنترنت، بما يحقق التوازن بين المصالح التي تبدو متنافسة في ظاهرها، ومن خلال تزويد المؤسسة، بما تحتاج إليه من الموظفين من ذوي الدراية والخبرة، ويجب - على أقل تقدير - أن يكون لدى وزارة الخارجية، الموارد اللازمة؛ لتنسيق المواقف، عبر جميع فروع الحكومة، ومصاحبة الوفود كافة، كما يجب استحداث وظائف بدوام كامل، أو نقاط اتصال تابعة للوزارة، لدى الوكالات الأخرى ذات الصلة بذلك، والاستثمار المطلوب ضئيل نسبياً، لكن المنافع ستكون هائلة.

وبعد أن تم تأكيد أن الجنرال كيث ألكسندر، سيترأس القيادة الإلكترونية، وترقيته إلى رتبة جنرال ذي أربعة نجوم، فإن جهود وزارة الدفاع، في مجال الفضاء الإلكتروني، أصبح يقودها المسؤول الذي يحلّ في المرتبة الخامسة عشرة، على سلم التدرج الوظيفي بالوزارة، ومع إنشاء القيادة الإلكترونية، ضمن وزارة الدفاع، ينبغي منح مسألة الدبلوماسية الإلكترونية في وزارة الخارجية، الدرجة نفسها من الأهمية؛ وتحقيقاً لذلك، فإن على الكونجرس، أن يستحدث مكتباً للشؤون الإلكترونية، يتبع وكيل وزارة الخارجية للشؤون السياسية، وتكون من مهماته، الإشراف على: مؤسسات وزارة الخارجية المسؤولة - حالياً - عن مسائل الاتصالات الدولية، وحرية الإنترنت، والأمن الإلكتروني، وتشمل تلك المؤسسات: مكتب الشؤون الإلكترونية في الاستخبارات والبحوث، وهو المسؤول عن تحليل المسائل ذات الصلة بالأمن الإلكتروني، والتنسيق بين الوكالات والشؤون الدولية، والمجموعة المعنية بسياسات الاتصالات والمعلومات، ضمن مكتب شؤون الاقتصاد والطاقة والأعمال، وفرقة العمل المعنية بالحرية العالمية للإنترنت.

استحداث منتدى مركزي للقطاع الخاص لتنسيق أجندات حوكمة الإنترنت مع الحكومة الأمريكية

ينبغي لمكتب الشؤون الإلكترونية الجديد، أن يضمّ - كذلك - اللجان الاستشارية القائمة، ضمن وزارة الخارجية، إزاء ما يخصّ تكنولوجيا المعلومات؛ ومن ذلك: اللجنة

الاستشارية حول سياسات الاتصالات والمعلومات الدولية، واللجنة الاستشارية للاتصالات الدولية، وعلاوة على ذلك، لا بد من تشكيل لجنة جديدة، تركز - تحديداً - على الأمن الإلكتروني، وينبغي أن يخدم مكتب وحيد، تلك اللجان، بحيث يوفر منتدى مركزياً للقطاع الخاص؛ كي ينسق أجندات حوكمة الإنترنت، مع الحكومة الأمريكية، وتُعَدّ الشركات الأمريكية؛ من قبيل: مايكروسوفت، وسيمانتك، من الفاعلين المهمين في منتديات حوكمة الإنترنت، وفي الوقت الحاضر، نجد أن تلك الشركات، تتحمل جزءاً كبيراً من الحمل، وتفتقر إلى توجه واضح، بشأن كيفية النهوض بالمصالح القومية للولايات المتحدة، ومع أن مواقف الشركات الأمريكية، لا تتناسق وموقف الحكومة دائماً، فإن تلك الشركات، يجب أن تتاح لها الفرصة - مع ذلك - كي تشكل ذلك الموقف، وتفهم الأجندة التي تدعو الحكومة الأمريكية إليها.

زيادة التمويل للتواصل ومنتديات حوكمة الإنترنت

إن تعيين مسؤول كبير في البيت الأبيض؛ لشؤون حوكمة الإنترنت، واستحداث مكتب جديد، داخل وزارة الخارجية؛ لإدارة هذه القضية، لا يعنيان أن الوكالات الأخرى، ليس لها مصلحة، أو أنها لا يجوز أن تضطلع بدور، في التواصل الدولي، بشأن حوكمة الإنترنت، بل على العكس؛ فوزارات: الدفاع، والتجارة، والعدالة، والأمن الوطني - وكذلك: كيانات تابعة للوزارات؛ مثل: الإدارة الوطنية للاتصالات والمعلومات، ومكتب التحقيقات الاتحادي - ستواصل العمل، ضمن شراكات نشيطة: متعددة الأطراف وثنائية، ولكنها ستفعل ذلك، ضمن نظام، ينهض بجدول العمل الشامل للولايات المتحدة، ولا بد أن تكون مكاتبها المعنية بالشؤون الدولية، أو الكيانات المتواصلة ومنتديات حوكمة الإنترنت، مزودة بما يناسبها من الموظفين ذوي المستوى العالي الكافي، وأن يكون لديها: الوقت والموارد؛ للاستعداد للتواصل، وفي الوقت الراهن، فإن حوكمة الإنترنت، ليست من الأعمال التي يمكن الجميع امتهانها.

الخاتمة

إن الإنترنت تقف عند نقطة حاسمة، في تاريخها القصير نسبياً؛ فالأعمال الشريرة التي يقوم بها المجرمون والجواسيس والمحاربون، تهدد النمو والكفاءة الاقتصاديين اللذين تمخض عنهما، وجود شبكة عالمية وحيدة وتبادلية، وإذا لم تتم معالجة تلك التهديدات، على نحو بنّاء، من خلال مشاركة أمريكية ذات نطاق أوسع، فإن دولاً أخرى، ستدخل الساحة، وقد تصوغ حلاً، من شأنه: حرمان الإنترنت من الخصائص ذاتها التي أكسبتها القيمة في المقام الأول؛ وبأخذ تلك العوامل في الحسبان، فإن على الولايات المتحدة أن تتجاوز معارضتها التقليدية للتواصل، إزاء ما يتعلق بمسائل حوكمة الإنترنت، وأن تقود الجهود بين الدول ذات التوجهات المتشابهة؛ لتبديد الهواجس الأمنية؛ بوسائل من شأنها: تعزيز الإنترنت؛ بوصفها محركاً للنمو الاقتصادي، لا الانتقاص منها، وعلى الولايات المتحدة، أن تعمل على استحداث آليات دولية جديدة؛ لوقف الهجمات الإلكترونية، وملاحقة منفِّذي تلك الهجمات، وكبح الدول الضالعة في النشاط الضار؛ وهذه الجهود - إلى جانب الاستثمارات الرامية إلى إعادة هيكلة البروتوكولات الأساسية للإنترنت؛ لجعلها أكثر أمناً - يمكن أن تحفظ القيمة الاقتصادية المستقاة، من الإنترنت، وتوسِّع نطاقها.

الهوامش

1. انظر:

"Unsecured Economies: Protecting Vital Information," McAfee, January 21, 2009, http://www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html.

2. انظر:

Virtually Here: The Age of Cyber Warfare, McAfee Virtual Criminology Report, 2009, p. 13.

3. انظر:

Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, October 21, 2007.

4. انظر:

Stewart Baker, Shaun Waterman, and George Ivanov, *In the Crossfire: Critical Infrastructure in the Age of Cyber War* (Santa Clara, CA: McAfee, 2010).

5. بحسب تعريف القانون الاتحادي، فإن مصطلح "الإنترنت"، يشير إلى الشبكة الحاسوبية الدولية المكونة من شبكات بيانات اتحادية وغير اتحادية، قابلة للتشغيل المتبادل، وتعمل بتقنية تحويل الطرود: [أجزاء المعطيات الرقمية المراد نقلها] packet switching.

6. انظر:

Jeremy Malcolm, *Multi-stakeholder Governance and the Internet Governance Forum* (Perth: Terminus Press, 2008), p. 32.

7. «يدعو إعلان سلفادور، إلى إصلاح العدالة الجنائية؛ لتأمين حقوق الإنسان والأمن والتنمية»، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 19 نيسان/ إبريل 2010. انظر الموقع الشبكي:

http://www.unodc.org/southerncone/en/frontpage/2010/04/19-declaracao-de-salvadorpede-uma-reforma-da-justica-criminal-para-proteger-os-direitos-humanos-aseguranca-e-o-desenvol vimento.html.

8. انظر:

UN System Chief Executives Board for Coordination, First Regular Session of 2010, UNIDO Headquarters, Vienna, April 9, 2010, pp. 11-12.

9. انظر:

"Connecting America: The National Broadband Plan," Federal Communications Commission, March 15, 2010, p. xi, http://download.broadband.gov/plan/national broadband-plan.pdf.

10. للاطلاع على نقاش معمّق حول هذه المسألة، انظر:

Robert K. Knake, "Untangling Attribution: Moving to Accountability in Cyberspace," testimony before the House of Representatives Committee on Science and Technology, July 15, 2010, http://www.cfr.org/publication/22630/untangling_attribution.html.

11. هذا المفهوم، طوَّره جيسون هيلي، من رابطة دراسات الصراعات الإلكترونية، في:

"Beyond Attribution: A Vocabulary for National Responsibility for Cyber Attacks," April 1, 2010, http://www.cyberconflict.org/ccsa-in-the-news/jasonhealeyslatestpaper.

12. انظر:

"Cybercrime Convention: A Positive Beginning to a Long Road Ahead," *Journal of High Technology Law*, vol. 2, no. 1, 2003, p. 110.

13. انظر:

Council of Europe, "Convention on Cybercrime," CETS No. 185, July 1, 2004, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

14. انظر:

Financial Action Task Force, "About the Financial Action Task Force," http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1_1,00.html.

15. للاطلاع على نبذة عامة عن فرقة العمل المعنية بالعمل المالي، انظر:

"An Introduction to FATF and Its Work," FATF-GAFI, 2010, http://www.fatf-gafi.org/dataoecd/48/11/45139480.pdf.

16. للاطلاع على المزيد من المعلومات، حول مجموعة أدوات الاتحاد الدولي للاتصالات، بشأن تشريعات الجريمة الإلكترونية، انظر:

"ITU Cybercrime Legislation Resources: ITU Toolkit for Cybercrime Legislation," International Telecommunications Union, http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html.

17. انظر:

Oxford Internet Institute, "Mapping and Measuring Cybercrime (Invited Forum)," University of Oxford, January 22, 2010, http://www.oii.ox.ac.uk/events/?id=337.

18. ينظر مجلس الشيوخ الأمريكي، في اعتماد نهج أحادي، ويقضي قانون الإبلاغ عن الجريمة الإلكترونية الدولية والتعاون بشأنها، أن يقدِّم الرئيس تقويماً سنوياً، حول الجريمة الإلكترونية الدولية، وأن يعلِّق المساعدات والتمويل والبرامج التجارية؛ على أساس تلك النتائج، ولمشروع القانون، وهو الذي

اشترك في تقديمه، كلٌّ من: كيرستن جيليبراند (السيناتورة الديمقراطية عن نيويورك)، وأورين هاتش (السيناتور الجمهوري عن يوتا)، ميزاته، ولكنه يخفق في أحد الجوانب المهمة؛ فهو لا يقوِّم أحد أكبر ملاذات مجرمي الإنترنت - أي الولايات المتحدة - بما يقلِّص احتمال أن يكون له التأثير الفاضح المطلوب، وعلاوة على ذلك، فإن أي عقوبات تفرضها الولايات المتحدة؛ بناءً على تلك التصنيفات، لا يُحتمل أن يكون لها التأثير المطلوب، في الدول المستهدفة، من حيث تحسّن سلوكها.

19. انظر:

Richard Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010).

20. انظر:

The White House, *The National Strategy to Secure Cyberspace*, February 2003, p. 30.

21. Ibid.

22. انظر:

Marcus H. Sachs, *Who e-Governs?* George Mason University, Policy Analysis Research Paper, December 4, 2007, p. 14.

23. انظر:

"Mike McConnell on How to Win the Cyber War We're Losing," *Washington Post*, February 28, 2010.

قواعد النشر

أولاً: القواعد العامة

1. تقبل للنشر في هذه السلسلة البحوث المترجمة من اللغات الأجنبية المختلفة، وكذلك الدراسات التي يكتبها سياسيون وكتاب عالميون.
2. يُشترط أن يكون البحث المترجم أو الدراسة في موضوع يدخل ضمن اهتمامات المركز.
3. يشترط ألا يكون قد سبق نشر الدراسة أو نشر ترجمتها في جهات أخرى.
4. تصبح الدراسات والبحوث المنشورة في هذه السلسلة ملكاً لمركز الإمارات للدراسات والبحوث الاستراتيجية، ولا يحق للمترجم أو المؤلف إعادة نشرها في مكان آخر.
5. يتولى المركز إجراءات الحصول على موافقة الناشرين الأصليين للبحوث المترجمة.

ثانياً: إجراءات النشر

1. تقدم الدراسة أو الترجمة مطبوعة من نسخة واحدة.
2. ترفق مع الترجمة صورة من المقالة باللغة المترجم عنها، وبيانات عن المصدر الذي أخذت منه.
3. يرسل مع البحث أو الترجمة بيان موجز بالسيرة العلمية للمترجم أو للباحث.
4. تقوم هيئة التحرير بمراجعة البحث أو الترجمة للتأكد من مستواهما، من خلال مراجعين من ذوي الاختصاص.
5. يخطر الباحث أو المترجم بنتيجة المراجعة خلال ثلاثة أشهر من تاريخ تسلم البحث.
6. تتولى هيئة التحرير المراجعة اللغوية وتعديل المصطلحات بما لا يخل بمضمون البحث أو الترجمة.

صدر من سلسلة «دراسات عالمية»

1. نحو شرق أوسط جديد، إعادة النظر في المسألة النووية — أفنر كوهين
2. السيطرة على الفضاء في حرب الخليج الثانية وما بعدها — ستيفن لمباكيس
3. النزاع في طاجكستان، التفاعل بين التمزق الداخلي والمؤثرات الخارجية (1991 - 1994) — جوليان ثوني
4. حرب الخليج الثانية، التكاليف والمساهمات المالية للحلفاء — ستيفن داجت، جاري جي. باجليانو
5. رأس المال الاجتماعي والاقتصاد العالمي — فرانسيس فوكوياما
6. القدرات العسكرية الإيرانية — أنتوني كوردزمان
7. برامج الخصخصة في العالم العربي — هارفي فيجنباوم وجفري هينج وبول ستيفنز
8. الجزائر بين الطريق المسدود والحل الأمثل — هيو روبرتس
9. المشكلات القومية والعرقية في باكستان — أبها دكسيت
10. المناخ الأمني في شرق آسيا — سنجانا جوشي
11. الإصلاح الاقتصادي في الصين ودلالاته السياسية — وي وي زانج
12. السياسة الدولية في شمال شرق آسيا... المثلث الاستراتيجي: الصين - اليابان - الولايات المتحدة الأمريكية — توماس ويلبورن
13. رؤية استراتيجية عامة للأوضاع العالمية — إعداد: إيرل تيلفورد
14. العراق في العقد المقبل: هل سيقوى على البقاء حتى عام 2002؟ — جراهام فولر
15. السياسة الخارجية الأمريكية بعد انتهاء الحرب الباردة — دانيال وارنر
16. التنمية الصناعية المستديمة — ديفيد والاس
17. التحولات في الشرق الأوسط وشمال إفريقيا: التحديات والاحتمالات أمام أوربا وشركائها — فيرنر فاينفلد ويوزيف يانج وسفن بيرنيد
18. جدلية الصراعات العرقية ومشروعات النفط في القوقاز — فيكن تشيتريان
19. العلاقات الدفاعية والأمنية بين إنجلترا وألمانيا «نظرة تقويمية» — إدوارد فوستر وبيتر شميت

صدر من سلسلة «دراسات عالمية»

.20	اقتصادات الخليج: استراتيجيات النمو في القرن الحادي والعشرين	تحرير: جوليا ديفلين
.21	القيم الإسلامية والقيم الغربية	علي الأمين المزروعي
.22	الشراكة الأوربية – المتوسطية: إطار برشلونة	آر. كيه. رامازاني
.23	رؤية استراتيجية عامة للأوضاع العالمية (2)	إعداد: إيرل تيلفورد
.24	النظرة الآسيوية نحو دول الخليج العربية	كيه. إس. بلاكريشنان جوليوس سيزار بارينياس جاسجيت سنج فيلوثفار كاناجا راجان
.25	سياسة أوربا الخارجية غير المشتركة	فيليب جوردون
.26	سياسة الردع والصراعات الإقليمية المطامح والمغالطات والخيارات الثابتة	كولن جراي
.27	الجرأة والحذر في سياسة تركيا الخارجية	مالك مفتي
.28	العولمة الناقصة: التفكك الإقليمي والليبرالية السلطوية في الشرق الأوسط	يزيد صايغ
.29	العلاقات التركية – الإسرائيلية من منظور الجدل حول الهوية التركية	م. هاكان يافوز
.30	الثورة في الشؤون الاستراتيجية	لورنس فريدمان
.31	السيطرة السريعة: ثورة حقيقية في الشؤون العسكرية التقنيات والنظم المستخدمة لتحقيق عنصري الصدمة والترويع	هارلان أولمان وجيمس بي. ويد
.32	التيارات السياسية في إيران 1981 - 1997	تأليف: سعيد برزين ترجمة: علاء الرضائي
.33	اتفاقيات المياه في أوسلو 2: تفادي كارثة وشيكة	ألوين روير
.34	السياسة الاقتصادية والمؤسسات والنمو الاقتصادي في عصر العولمة	تيرنس كاسي

صدر من سلسلة «دراسات عالمية»

35. دولة الإمارات العربية المتحدة الوطنية والهوية العربية - الإسلامية	سالي فندلو
36. استقرار عالم القطب الواحد	وليم وولفورث
37. النظام العسكري والسياسي في باكستان	تأليف: إيزابيل كوردونير ترجمة: عبدالله جمعة الحاج
38. إيران بين الخليج العربي وحوض بحر قزوين الانعكاسات الاستراتيجية والاقتصادية	شيرين هنتر
39. برنامج التسلح النووي الباكستاني نقاط التحول والخيارات النووية	سمينة أحمد
40. تدخل حلف شمال الأطلسي في كوسوفا	ترجمة: الطاهر بوساحية
41. الاحتواء المزدوج وما وراءه: تأملات في الفكر الاستراتيجي الأمريكي	عمرو ثابت
42. الصراع الوطني الممتد والتغير في الخصوبة: الفلسطينيون والإسرائيليون في القرن العشرين	فيليب فرج
43. مفاوضات السلام وديناميية الصراع العربي - الإسرائيلي	عمرو جمال الدين ثابت
44. نفط الخليج العربي: الإنتاج والأسعار حتى عام 2020	ديرموت جيتلي
45. انهيار العملية السلمية الفلسطينية - الإسرائيلية: أين الخلل؟	جيروم سليتر
46. ثورة المعلومات والأمن القومي	تحرير: توماس كوبلاند
47. القانون الدولي والحرب ضد الإرهاب	كريستوفر جرينوود
48. إيران والعراق	تشاس فريمان (الابن) وآخرون
49. إصلاح نظم حقوق الملكية الفكرية في الدول النامية: الانعكاسات والسياسات	طارق علما ومايا كنعان
50. الأسطورة الخضراء: النمو الاقتصادي وجودة البيئة	ماريان رادتسكي

صدر من سلسلة «دراسات عالمية»

	العنوان	المؤلف
51.	التصورات العربية لتركيا وانحيازها إلى إسرائيل بين مظالم الأمس ومخاوف اليوم	أوفرا بنجيو وجنسر أوزكان
52.	مستقبل الأيدز: الحصيلة المروعة في روسيا والصين والهند	نيكولاس إيبراشتات
53.	الدور المتغير للمعلومات في الحرب	تحرير: زلمي خليل زاد وجون وايت
54.	مسؤولية الحماية وأزمة العمل الإنساني	جاريث إيفانز ومحمد سحنون وديفيد ريف
55.	الليبرالية وتقويض سيادة الإسلام	عمرو ثابت
56.	الوفاق الهندي - الإسرائيلي	أفرايم إنبار
57.	الفضائيات العربية والسياسة في الشرق الأوسط	محمد زياني
58.	دور تصدير المياه في السياسة الإيرانية الخارجية تجاه مجلس التعاون لدول الخليج العربية	كامران تارمي
59.	أهمية النجاح: الحساسية إزاء الإصابات والحرب في العراق	كريستوفر جيلبي وآخران
60.	الفوز مع الحلفاء: القيمة الاستراتيجية للنموذج الأفغاني	ريتشارد أندريس وآخران
61.	الخروج من العراق: استراتيجيات متنافسة	توماس ماتير
62.	آراء من داخل الشبكة: تأثير المواقع الإلكترونية في الاهتمامات السياسية للشبان	آرثر لوبيا و تاشا فيلبوت
63.	دبلوماسية الصين النفطية في إفريقيا	أيان تايلر
64.	التدخل العسكري والأسلحة النووية: حول المبدأ الأمريكي الجديد بشأن استخدام السلاح النووي	هارالد مولر و شتيفاني زونيوس ترجمة: عدنان عباس علي
65.	العقوبات في السياسة الدولية: نظرة على نتائج الدراسات والأبحاث	بيتر رودولف ترجمة: عدنان عباس علي
66.	اللوبي الإسرائيلي والسياسة الخارجية الأمريكية	جون ميرشايمر وستيفن والت

صدر من سلسلة «دراسات عالمية»

صدر من سلسلة «دراسات عالمية»

العنوان	المؤلف
77. إعادة التفكير في المصلحة القومية واقعية أمريكية من أجل عالم جديد	كونددوليزا رايس
78. الصين المتغيرة: احتمالات الديمقراطية في الداخل والدبلوماسية الجديدة تجاه "الدول المارقة"	جون ثورنتون وستيفاني كلين – ألبراندت وأندرو سمول
79. التوجه الجديد لليبيا	مولفريد بروت – هيجهامر ورونالد بروس سانت جون
80. أزمة الغذاء العالمية	أليكس إيفانز ويواخيم فون براون وآخرون
81. عهد أوباما سياسة أمريكية للشرق الأوسط	ريتشارد هاس ومارتن أنديك ووالتر راسل ميد
82. اللوبي الهندي والاتفاقية النووية الأمريكية – الهندية	جيسون أ. كيرك
83. وقت الإغلاق: التهديد الإيراني لمضيق هرمز	كيتلين تالماج
84. دور حكام الولايات في السياسة الخارجية الأمريكية	صامويل لوكاس ماكميلان
85. الأزمة المالية العالمية	بن ستيل وستيفن دوناواي
86. شرق إفريقيا: الأمن وإرث الهشاشة	جيلبرت خادياجالا
87. المتعاقدون في الحروب	مارك كانسيان وستيفن شونر
88. الثقافة الاستراتيجية الإيرانية والردع النووي	جنيفر كنيبر وأندرو تيريل
89. أمن الطاقة الأوراسية	جفري مانكوف
90. أسلحة الدمار الشامل والأسلحة الصغيرة والخفيفة: فرق عمل تعزيز القدرات الأمنية المتعددة الأطراف	معهد السلام الدولي
91. هل التقسيم حلٌ للحرب الأهلية؟	نيكولاس سامبانس وجونا شولهوفر-ول
92. الصراعات في أقاليم الصومال	سولومون ديرسو وبيروك مسفين

صدر من سلسلة «دراسات عالمية»

93. الغرب وروسيا في البحر الأبيض المتوسط: نحو تنافس متجدد! — ديريك لوتربيك وجورجي إنغلبريخت
94. ما بعد الدولار: إعادة التفكير في النظام النقدي الدولي — باولا سوباتشي وجون دريفل
95. حوكمة الإنترنت في عصر انعدام الأمن الإلكتروني — روبرت كنيك

قسيمة اشتراك في سلسلة

«دراسات عالمية»

الاسم : ....

المؤسسة : ....

العنوان : ....

ص. ب : .... المدينة: ....

الرمز البريدي: ....

الدولة : ....

هاتف : .... فاكس: ....

البريد الإلكتروني: ....

بدء الاشتراك: (من العدد: .... إلى العدد: ....)

رسوم الاشتراك*

للأفراد:	220 درهماً	60 دولاراً أمريكياً
للمؤسسات:	440 درهماً	120 دولاراً أمريكياً

- ❑ للاشتراك من داخل الدولة يقبل الدفع النقدي، والشيكات، والحوالات النقدية.
- ❑ للاشتراك من خارج الدولة تقبل فقط الحوالات المصرفية، مع تحمل المشترك تكاليف التحويل.
- ❑ في حالة الحوالة المصرفية، يرجى تحويل قيمة الاشتراك إلى حساب مركز الإمارات للدراسات والبحوث الاستراتيجية رقم 1950050565 ـ بنك أبوظبي الوطني ـ فرع الخالدية. ص. ب: 46175 أبوظبي ـ دولة الإمارات العربية المتحدة.
- ❑ يمكن الاشتراك عبر موقعنا على الإنترنت (www.ecssr.ae) باستعمال بطاقتي الائتمان Visa و Master Card.

لمزيد من المعلومات حول آلية الاشتراك يرجى الاتصال:

مركز الإمارات للدراسات والبحوث الاستراتيجية

قسم التوزيع والمعارض

ص.ب: 4567 أبوظبي ـ دولة الإمارات العربية المتحدة

هاتف: 4044445(9712) فاكس: 4044443(9712)

البريد الإلكتروني: books@ecssr.ae

الموقع على الإنترنت: http://www.ecssr.ae

* تشمل رسوم الاشتراك الرسوم البريدية، وتغطي تكلفة اثني عشر عدداً من تاريخ بدء الاشتراك.

حوكمة الإنترنت

في عصر انعدام الأمن الإلكتروني

مركز الإمارات للدراسات والبحوث الاستراتيجية

أنشئ مركز الإمارات للدراسات والبحوث الاستراتيجية في أبوظبي بتاريخ 14 آذار/ مارس 1994، كمؤسسة بحثية مستقلة تعنى بدراسة القضايا الاستراتيجية السياسية والاقتصادية والاجتماعية والمعلوماتية، التي تهم دولة الإمارات العربية المتحدة ومنطقة الخليج العربي خصوصاً والعالم العربي عموماً، ومتابعة أهم المستجدات الإقليمية والدولية.

وفي إطار التفاعل الثقافي والتعاون العلمي، يصدر المركز سلسلة **دراسات عالمية** التي تعنى بترجمة أهم الدراسات والبحوث التي تنشر في دوريات عالمية مرموقة، وتتصل موضوعاتها باهتمامات المركز العلمية، كما تهتم بنشر البحوث والدراسات بأقلام مشاهير الكتاب ورجال السياسة.

ويرحب المركز بتلقي البحوث والدراسات المترجمة، وفق قواعد النشر الخاصة بالسلسلة.

دراســات عــالميــة

حوكمة الإنترنت في عصر انعدام الأمن الإلكتروني

روبرت كنيك

العـدد 95

تصـدر عن





محتوى الدراسة لا يعبر بالضرورة عن وجهة نظر المركز

This is an authorized translation of the Council Special Report no. 56 (September 2010), entitled "Internet Governance in an Age of Cyber Insecurity" by Robert K. Knake and published by Council on Foreign Affairs. The ECSSR is indebted to the author and to the publisher for permitting the translation, publication and distribution of this work under its name.

الطبعة الأولى 2011

ISSN 1682-1211

النسخة العادية ISBN 978-9948-14-412-0

النسخة الإلكترونية ISBN 978-9948-14-413-7

توجه المراسلات باسم رئيس تحرير سلسلة **دراسات عالمية**

على العنوان التالي:

مركز الإمارات للدراسات والبحوث الاستراتيجية

ص ب: 4567

أبوظبي، دولة الإمارات العربية المتحدة

هاتف: +9712-4044541

فاكس: +9712-4044542

E-mail: pubdis@ecssr.ae

Website: http://www.ecssr.ae

المحتويـات

تمهيد

أحدثت الإنترنت، منذ بدايتها عام 1989، ثورة في التجارة والاتصالات والعمل العسكري والحوكمة، ولم يعد من الممكن - ببساطة - تصور جزء كبير من العالم المعاصر من دونها، بيد أن تلك الثورة لم تكن من دون ثمن؛ فالتكلفة السنوية للجرائم الإلكترونية، [أو السبرانية؛ أي عبر الإنترنت]، تفوق الآن تريليون دولار، بينما شلَّت الهجمات الإلكترونية المنسَّقة، كلاًّ من: أستونيا وجورجيا وقرغيزستان، وألحقت الضرر ببنى أساسية حسّاسة، في دول مختلفة حول العالم، وبينما سعى ما لا يقل عن ستة من أجهزة الأمم المتحدة، والكثير من المنتديات الإقليمية والوطنية، للتوصل إلى توافق آراء، حول مستقبل حوكمة الإنترنت، [أو إدارتها]، فإنه لم يُحرَز إلا تقدم ضئيل في هذا المضمار حتى الآن، وقد امتنعت الولايات المتحدة الأمريكية بنفسها - إلى حد بعيد - عن هذه المناقشات، وركَّزت، بدلاً من ذلك، على تطوير قدراتها الهجومية والدفاعية، في مجال الأمن الإلكتروني، مع الاعتماد على خبرات القطاع الخاص؛ للمحافظة على استمرار استقرار النظام.

يتفحص روبرت كنيك، في هذا التقرير، القرارات التكنولوجية التي أتاحت النجاح الباهر للإنترنت، وجعلتها - في الوقت ذاته - عرضة للهجمات، على نحو يثير القلق! ويرى المؤلف أن الولايات المتحدة، لم يعد بإمكانها أن تتخلى عن زمام المبادرة، في المسائل الإلكترونية، لمصلحة دول لا تشاركها المصالح، ويرسم المؤلف الخطوط العريضة، للأجندة التي يمكن أن تسعى لتحقيقها، بالتنسيق بينها وبين حلفائها على الصعيد الدولي، ويضيف: أن تلك الأجندة - وهي التي تعالج مسائل الحرب الإلكترونية، والجريمة الإلكترونية، والتجسس الذي ترعاه الدول - ينبغي السعي لتحقيقها، باستخدام الأساليب التكنولوجية والقانونية معاً، وهو يحثّ الولايات المتحدة على أن تبدأ بدعم الخبراء، بما يمكّنهم من التصدي للمسائل الأمنية الأساسية التي تكمن في صلب تصميم الإنترنت، ثم يحدد الأدوات القانونية الضرورية؛ لمعالجة مسألتي: الجريمة الإلكترونية، والنشاطات التي ترعاها الدول؛ ومن ذلك: تدابير منع الجريمة الإلكترونية، على المستوى

الوطني، والآليات المتعددة الأطراف؛ لمنع الهجمات الإلكترونية، وملاحقة مرتكبيها، وقواعد حماية النظم المدنية الحساسة في زمن السلم، ويصف - من بعد ذلك - الإصلاحات البيروقراطية التي يتعين على الولايات المتحدة القيام بها؛ للتنفيذ الفعّال لتلك التغييرات.

وتقرير **حوكمة الإنترنت في عصر انعدام الأمن الإلكتروني**، إسهام يأتي في حينه، حول مسألة، تستحوذ بصورة متزايدة، على اهتمام صانعي السياسات، وهو يقدِّم أفكاراً تقنية لغير الخبراء، بلغة سهلة وجذابة، والتقرير لا يَدَع مجالاً للشك، في أهمية الأمن الإلكتروني، بالنسبة إلى مستقبل الولايات المتحدة، ومستقبل الإنترنت ذاتها، وتوفِّر توصياته، أساساً قوياً، يُستند إليه، إزاء ما سيتم اتخاذه من تدابير في المستقبل.

ريتشارد هاس

رئيس مجلس العلاقات الخارجية

أيلول/ سبتمبر 2010

كلمة شكر

لم يكن هذا التقرير ليرى النور؛ لولا استفادته من الخبرة والمشورة والصبر لدى لجنته الاستشارية؛ ذلك أن كل عضو من أعضائها، لديه من الخبرة في هذه المسائل، ما يفوق بكثير إسهامي في هذا المشروع، وأنا أدين لهم بالعرفان؛ لقبولهم إتاحة الاستفادة من تلك الخبرة، وتحمُّلهم عناء قراءة المسودات الكثيرة للتقرير، وأما الأخطاء الوقائعية أو المنطقية، وهي التي قد تكون ماتزال قائمة، فإنما تعود مسؤوليتها إلي وحدي.

فقد أدّت إستر دايسون، مهمة رائعة، من خلال ترؤسها اجتماعات اللجنة الاستشارية، وإتاحتها - في الوقت ذاته - الاستفادة من آرائها النقدية، والخبرة التي اكتسبتها، على مدى عقود، داخل مجتمع حوكمة الإنترنت، وأدين بالشكر لريتشارد هاس، رئيس مجلس العلاقات الخارجية، وللجنة جمعية الشؤون الخارجية بالمجلس؛ للفرصة التي مُنحتها؛ كي أمضي عاماً من العمل، على وضع سياسة، إزاء ما يخصّ الأمن الإلكتروني، والشكر موصول - أيضاً - إلى جيمس ليندسي، النائب الأول لرئيس المجلس، ومدير الدراسات، وأستاذ كرسي موريس آر جرينبرج؛ للدعم الذي شمل به المشروع، إلى أن رأى النور؛ وللصبر الذي تحلّى به، لدى مراجعة مسودات عدّة، إلى أن اتضحت اللغة، واستبانت المصالح القومية للولايات المتحدة.

وقد وفّر لي برنامج الشركات،* وبرنامج الكونجرس** للمجلس، الفرصة؛ كي اختبر الأفكار المتضمَّنة في هذا التقرير، في حضور لفيف من الخبراء، قبل نشره؛ فتحسَّن التقرير كثيراً؛ بفضل التعليقات التي تلقّيتها في كل جلسة، وقد دعاني جيمس لويس، من مركز الدراسات الاستراتيجية والدولية، إلى المشاركة في اجتماعات مع معهد العلاقات الدولية المعاصرة في الصين؛ حيث اكتسبت فهماً قيّماً مباشراً، لأهداف ذلك البلد، وغاياته، على صعيد حوكمة الإنترنت.

---

* لقاءات تفاعلية بين أعضاء المجلس وقادة الأعمال والمال بشأن التحديات الدولية المهمة. (المترجم)

** ملتقيات إحاطة ونقاش مع أعضاء الكونجرس وصانعي السياسات في واشنطن. (المترجم)

وأودّ أن أتوجه بالشكر، لجون رولينز، في قسم أبحاث الكونجرس؛ لمساعدتي على فهم دور الكونجرس في حوكمة الإنترنت، ولفينس كريسلر، من شركة زايكنر ريسك آناليتيكس المحدودة؛ لتقديمه فهماً قيّماً لتحديات السياسات، ومشورة تقنية، كنت أحوج ما أكون إليها، بشأن الآليات الداخلية للإنترنت، كما أشعر بالامتنان - كذلك - نحو رود بِكستروم، رئيس شركة الإنترنت للأسماء والأرقام المخصصة (ICANN)، وهو الذي حضر اجتماعنا الاستشاري الأول، في إطار اللجنة، وأطلعنا على تصوّره، وقد وافاني آدم سيجال، وهو زميل أول بالمجلس، بتقويماته باستمرار، وخصَّص جزءاً من وقته؛ لمساعدتي على إعادة تنظيم المسودة النهائية للتقرير، وعلى التركيز على المصالح القومية الأمريكية، في الفضاء الإلكتروني، والسبل المثلى لتحقيقها.

وأسهمت بريتي باتاشارجي، وهي باحثة مشاركة، في ضمان استمرار تقدُّم المشروع واكتماله، في الوقت المحدد، من خلال العناية بالتفصيلات كافة، على الوجه الأكمل، وساعدت لوسي داندرديل، وهي منسّقة الاتصال، على توجيهي، في أجواء مرحة، عبر مرحلة اعتماد التقرير، وساعدتني ريتشل هاريس، وهي متدربة سابقة في المجلس، على إجراء الأبحاث اللازمة؛ حيث عالجت بمهارة، طلبات صعبة، حول موضوعات غير شائعة.

وقد أُعدّ هذا التقرير، في إطار برنامج المؤسسات الدولية والحوكمة العالمية، الذي يقوده ستيوارت إم باتريك، وهو زميل أول؛ فقد قدَّم مشورة قيّمة، حول محتوى التقرير وبنيته، والمشروع أمكن تنفيذه؛ بفضل هبة سخية مقدَّمة من مؤسسة روبينا.

روبرت كنيك

مقدمة

لم تعد الولايات المتحدة، تتصدر الملتقيات الدولية التي ستحدد مستقبل الإنترنت؛ فالأنظمة غير الديمقراطية، بقيادة روسيا والصين، بدأت تنظم صفوفها؛ لتشكِّل جبهة موحدة تروِّج لرؤيةٍ للإنترنت، تتسم بإحكام الدول سيطرتها عليها، وهذه الرؤية تزداد جاذبيتها، لدى الكثير من الدول الأوربية التي تسعى جاهدة، لمعالجة تهديدات مترابطة، وممثلة بالجريمة الإلكترونية، والجاسوسية الصناعية، والحرب الإلكترونية، وعلى الولايات المتحدة، أن تكافح تلك التهديدات بنشاط، في الوقت الذي تعمل فيه، على حماية المصالح القومية الأمريكية الممثلة بالمحافظة على الإنترنت، وتوسيع نطاقها؛ بوصفها منصةً لزيادة الكفاءة والتبادل الاقتصادي، وحماية هذه المصلحة، تتطلب تواصلاً أوسع بكثير، ضمن ملتقيات حوكمة الإنترنت؛ لتشكيل مستقبل الشبكة، على نحو يبدد الهواجس الأمنية، من دون أن يتمخض عن دواء أسوأ من الداء.

وتحقيقاً لهذا الهدف، فإن على الولايات المتحدة، أن تسترشد بمبادئ ثلاثة: أولاً، عليها أن تعتمد "نهجاً شبكياً وموزَّعاً" لـ "مشكلة شبكية وموزَّعة"؛ لأنه ما من منتدى، يمكنه أن يعالج [وحده] هذه المجموعة من المسائل، وعلى الولايات المتحدة الأمريكية أن تسعى - بدلاً من ذلك - لإيجاد حلول، من خلال مشاركة واسعة النطاق، تشمل مجموعة عريضة من المنتديات، وعلى الولايات المتحدة ثانياً، أن تتحرك باتجاه مساءلة الدول عن تصرفاتها وتصرفات مواطنيها وأنظمتها في الفضاء الإلكتروني؛ فمع أن الولايات المتحدة، لا يجوز أن تتوقع أن تمنع الدولُ كل أشكال السلوكيات الخبيثة، فإن لها أن تتوقع أن تتولى تلك الدول، حماية شبكاتها بدرجة معقولة، وسنّ القوانين التي تعاقب الجريمة الإلكترونية الدولية، وإرساء الآليات التي تستجيب لطلبات المساعدة على إحباط الهجمات، والتحقيق فيها، وملاحقة مرتكبيها، وعلى الولايات المتحدة ثالثاً، أن تكون القدوة؛ إذ عليها أن تتخذ خطوات؛ لتنظيف شبكتها القومية، والحيلولة دون أن تُستغل أنظمتها في الهجمات الإلكترونية الدولية، ومنح التحقيقات الجنائية في الهجمات الإلكترونية مع الضحايا الأجانب الأولوية، وإيضاح أن الهدف الأساسي من جهودها العسكرية، في الفضاء الإلكتروني، إنما هو حماية الولايات المتحدة، والمحافظة على التواصل الدولي.

وهذه الأهداف، يجب تطبيقها، ضمن جدول ثلاثي الأجزاء؛ فالولايات المتحدة، عليها أن تعمل على تطوير مجموعة نظم دولية أقوى؛ لمكافحة الجريمة في الفضاء الإلكتروني؛ بما يتعدى اتفاقية مجلس أوربا الراهنة، [وهي الخاصة بالجرائم الإلكترونية]؛ لاستقطاب الدول غير الغربية، واستحداث آليات، تعمل في الوقت الحقيقي؛ [أي على الفور]؛ للتعاون على وقف الهجمات الإلكترونية الجارية، والتحري عن الهجمات عبر الحدود، بيد أن معالجة الجريمة الإلكترونية وحدها، لا تكفي لتأمين الفضاء الإلكتروني؛ فالدول يجب تقييدها - كذلك - من خلال استحداث قواعد جديدة، وليس على الولايات المتحدة أن تخشى الحديث عن هذه الموضوعات، بل عليها أن تبرم اتفاقيات؛ لحماية الوظائف الأساسية للإنترنت، ومنع هجمات حجب الخدمة الموزَّعة،* وعليها - أيضاً - أن تحيي الجهود؛ لتأمين التكنولوجيات الأساسية للإنترنت، وهي التي طُوِّرت قبل عقود؛ لغرض يختلف عن الغرض الذي تُستخدم اليوم من أجله.

وعلى الولايات المتحدة أخيراً، أن ترسي آليات ضمن حكومتها؛ لتحقيق تلك الجداول، وهناك حاجة إلى مستوى قيادة أقوى في البيت الأبيض؛ لضمان استمرار التركيز على المصالح القومية الأمريكية، من الوكالات المهتمة بكيفية تطوير الإنترنت، ولا بد من الارتقاء بمسألة حوكمة الإنترنت لدى وزارة الخارجية، بحيث يُعنى بها مكتب جديد، يركز على الشؤون الإلكترونية؛ على أن توكل إليه مهمة العمل؛ لتحسين أمن الفضاء الإلكتروني، من خلال المشاركة الدولية، كما يجب أن يُفسَح المجال أكثر، للقطاع الخاص؛ كي يبدي رأيه بشأن تلك الموضوعات والآليات التي يتم تطويرها؛ من أجل الشركات؛ كي تسهم في تشكيل السياسة الأمريكية، وتنسِّق مواقفها.

* أحد أشكال تلك الهجمات، إغراق الهدف - (وهو أحد المواقع الشبكية مثلاً) - بطلبات الاتصال الخارجية؛ فيؤدي هذا إلى عجزه عن الاستجابة، أو الاستجابة ببطء، بحيث يعد غير متاح. (المترجم)

معلومات أساسية

منذ الأيام الأولى للإنترنت، سعى أبرز مصمميها ومؤيديها، للحدّ من دور الحكومة، في تصميم الشبكة وعملها وإدارتها، ومع أن الإنترنت نتاج أبحاث، موّلتها الولايات المتحدة طوال عقود، فإن علماء الحاسوب الذين طوروا البروتوكولات التي تعمل الإنترنت؛ وفقها اليوم، صمّموها، بحيث لا توجد ضرورة لمشغّل مركزي للشبكة، وطوال العقود الثلاثة السابقة، نجحت إدارات رئاسية متعاقبة، في اعتماد نهج، يقوم على عدم التدخل في تطوير الشبكة؛ فيسمح هذا للإنترنت بالنمو من دون مشاركة حكومية، كان يمكنها أن تحدّ من توسعها المطّرد أو توقفه، وقد تم توسيع نطاق هذا النهج؛ ليشمل المشهد الدولي ككل؛ حيث حافظت الولايات المتحدة على السيطرة على مكوّن ضروري واحد من مكونات البنية الأساسية للإنترنت، تتعين إدارته بنشاط؛ أي نظام اسم النطاق Domain Name System، وأما ماعدا ذلك، فكان موقفها يقوم على أن دور الحكومات في إدارة الشبكة، يجب أن يبقى محدوداً؛ وقد أدّى ظهور الجريمة الإلكترونية، والتجسس الإلكتروني، وشبح الحرب الإلكترونية، إلى أن تمارس حكومات أجنبية كثيرة، السلطة السيادية على شبكاتها، وتضغط على المنظمات الدولية؛ كي تُعنى بتلك المسائل.

فهم التهديد

يُقدَّر الضرر الذي تلحقه الجريمة الإلكترونية بالاقتصاد العالمي، بما يزيد على تريليون دولار سنوياً؛[1] فالهجمات المتطورة التي تستهدف الملكية الفكرية، لشركات [مجلة] فورتشن **500**، أصبحت من الأمور الروتينية، وقد انخرطت الدول في المشهد الممتزج؛ حيث طوَّرت قدرات هجومية ودفاعية معاً، ضمن شكل جديد من أشكال سباقات التسلح، والولايات المتحدة، في طريقها إلى تدشين القيادة الإلكترونية، وهي قيادة قتالية جديدة، يوكل إليها الإشراف على العمليات الهجومية والدفاعية، في الفضاء الإلكتروني، ويترأسها جنرال بأربعة نجوم، وهناك أربع دول أخرى على الأقل، طوَّرت قدرات على القيام بعمليات إلكترونية هجومية متطورة، بينما شرع ما يزيد على مائة دولة، في تنظيم وحدات للحروب الإلكترونية.[2]

وتلك القدرات، لم تكن مقصورة على المختبرات؛ ففي عام 2007، تعرضت أستونيا لهجوم حجب الخدمة على المستوى الوطني؛ أدّى إلى أن يبقى البلد كله، مفصولاً عن الإنترنت على مدار أسبوع؛ فأثّر هذا في: الشبكات الحكومية، وشبكات الاتصالات، والدوائر المالية،[3] وبعد مضي عام، وعندما غزت روسيا جورجيا، سبق هجومٌ في الفضاء الإلكتروني القوات البرية والجوية، وتلك الصراعات المبكرة في الفضاء الإلكتروني، إنذارات محتملة بهجمات، أسوأ بكثير، وقد برهن الباحثون على القدرة على استخدام الهجمات الإلكترونية؛ لتدمير القيود المالية، وقطع التيار الكهربائي، وتعطيل الشبكات الضرورية للعمليات العسكرية، وأصبحت قطاعات رئيسية في مجال البنية الأساسية - ومنها قطاعات: الطاقة والنفط والغاز والمياه والصرف الصحي - مستهدفة على نحو متزايد.[4]

حوكمة الإنترنت اليوم

إن الإنترنت؛ بوصفها شبكة مؤلفة من شبكات، لا تخضع لسلطة مركزية،[5] والمعايير التقنية الجديدة للبروتوكولات التي تعمل الإنترنت وفقها، يتم تطويرها من خلال عملية "طلب تعليق"* تكرارية، تديرها فرقة العمل المعنية بهندسة الإنترنت،** ويعتمدها المجتمع التقني على أساس توافقي؛ وإدراكاً للحاجة إلى سلطة مركزية؛ لتخصيص معرِّفات identifiers، اسمية ورقمية فريدة، استحدث نظام اسم النطاق، في أوائل الثمانينيات من القرن العشرين، والدور الممثل بتخصيص عناوين بروتوكولات الإنترنت، وإدارة منطقة الجذر root zone: (أسماء وعناوين لبروتوكولات الإنترنت الخاصة بخوادم نظام أسماء النطاق المعتمدين أو المخوَّلين لجميع نطاقات المستوى الأعلى؛ من قبيل: "دوت كوم".com)، كان يضطلع به فرد واحد، يُدعى جون بوستل John Postel، مدة تقارب العقدين،[6] وفي عام 1998، استحدثت وزارة التجارة الأمريكية، شركة الإنترنت للأسماء والأرقام المخصصة ICANN؛ للإشراف على إدارة هذا النظام من المعرِّفات الفريدة.

---

* مذكرة تصدرها فرقة العمل المعنية بهندسة الإنترنت، تصف فيها: الأساليب أو السلوكيات أو الأبحاث أو الابتكارات التي يمكن تطبيقها، على عمل الإنترنت والنظم المتصلة بها. (المترجم)

** المنظمة الرئيسية المعنية بوضع المعايير الخاصة بالإنترنت، وهي مجتمع دولي كبير مفتوح، من المصممين والمشغّلين والباعة والباحثين المعنيين بتطوير بنية الإنترنت، وعملها بشكل سلس. (المترجم)

وتشغِّل شركة ICANN، النظام المركزي الوحيد الضروري لاستمرار عمل الإنترنت، وهي تضطلع بذلك الدور، بحجم تكلفة أدنى، وتتخذ التدابير؛ لمعالجة المسائل الأمنية التي تدخل ضمن نطاق ولايتها، ويرى الكثير من رواد الإنترنت ومن مؤيدي حريتها، أن تخصيص تلك المعرِّفات الفريدة، هو الوظيفة الضرورية الوحيدة، على صعيد حوكمة الإنترنت، وقد اتفقت إدارات أمريكية متعاقبة إلى حد كبير على هذا الرأي، وحدَّت من تدخل الحكومة الأمريكية، وسعت لكبح حكومات أخرى، إزاء محاولة ممارسة السلطة على الشبكة، بما يتيح للشبكة أن تنمو من دون عوائق، بيد أن الاتجاه المتصاعد للبرمجيات الضارة، وانتشار سرقات الهوية والجرائم المالية، واستخدام الإنترنت من الإرهابيين، والمستويات غير المسبوقة التي بلغها التجسس بين الشركات، وتطوُّر قدرات الدول في مجال الحرب الإلكترونية الهجومية، والاستغلال الإلكتروني، كلها عوامل، تشير إلى الضرورة المحتملة لنمط حوكمة أقوى وأشمل؛ كي تنمو الإنترنت، وتواصل إضافة قيمة إلى التجارة العالمية، وجعل الحياة اليومية للمليارات من البشر ثرية.

وبالنظر إلى تكاليف الجريمة والتهديد الاقتصادي للتجسس الصناعي وتزايد عسكرة الفضاء الإلكتروني، فإن نهج عدم التدخل الذي كانت الولايات المتحدة، تعتمده بشأن حوكمة الإنترنت، طوال العقد الماضي، لم يعد من الممكن إدامته، وعلى الرغم من أن الإنترنت التي نعرفها اليوم، هي نتاج مجهود تعاوني بين الحكومة الأمريكية، والقطاع الخاص، والمجتمع الأكاديمي، فإن حق المباهاة المتأتي من ملكية السبق التاريخي، لا يمتد إلى السيطرة على مستقبل الإنترنت؛ فإذا لم تتحلَّ الولايات المتحدة بالقيادة الضرورية؛ لمعالجة المشكلات الأمنية، فإن دولاً أخرى سوف تتولى ذلك، وإذا كانت الإنترنت بصورتها الحالية، تجسيداً للانفتاح والابتكار اللذين يتّسم بهما المجتمع الأمريكي، فإن الإنترنت المستقبلية - وفق تصور روسيا والصين - سوف تجسّد مجتمعيهما؛ أي ستكون منغلقة، ومعتلّة، وخاضعة لسيطرة الدولة، وواقعة تحت مراقبة مكثفة.

مبادرات حكومية دولية جديدة

وبالنظر إلى الهواجس الأمنية، نجد أن بلداناً كثيرة، تتعجّل اعتماد مبادرات جديدة؛ بهدف تأمين الفضاء الإلكتروني، في عدد ضخم من المنتديات الدولية التي تتسابق على الاضطلاع بدور في حوكمة الإنترنت؛ ومن ذلك: ما لا يقل عن ستة منتديات داخل الأمم المتحدة وحدها، كما تنشط - كذلك - مجموعات إقليمية؛ مثل: رابطة التعاون الاقتصادي لآسيا والمحيط الهادي، ومنظمة التعاون الاقتصادي والتنمية، ومنظمة الدول الأمريكية، وتمارس الحكومة الروسية، ضغوطاً منذ عام 1998؛ للتوصل إلى معاهدة - ضمن إطار الأمم المتحدة - تعالج الصراع في الفضاء الإلكتروني، وقد بدأت الفكرة تكتسب زخماً في الآونة الأخيرة، كما حظي المفهوم بالتأييد، في مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، وهو الذي عُقد في سلفادور، بالبرازيل، في نيسان/ إبريل عام 2010،[7] ويبذل حامادون توري Hamadon I. Touré، وهو الأمين العام للاتحاد الدولي للاتصالات، جهداً حثيثاً؛ للوصول إلى مثل ذلك الاتفاق، وقد دعا مؤخراً، إلى عقد مؤتمر للأمم المتحدة، يتولى وضع "مخطط لنهج على نطاق المنظومة"، إزاء ما يتعلق بأمن الفضاء الإلكتروني.[8]

ومن الواضح أن هذه النتيجة، تتناقض والمصالح الأمريكية؛ فالاتحاد؛ بوصفه منظمة، ليس مصمَّماً لإدارة مسائل معقدة؛ مثل: أمن الفضاء الإلكتروني، وهو غير مكلف بمعالجة مسائل؛ مثل: الجريمة، والصراعات بين الدول، كما أن الاتحاد؛ بوصفه منظمة دولية حكومية، عمادها الدول، ليس مصمَّماً، بحيث تشارك المنظمات غير الحكومية والقطاع الخاص في مناقشاته، أما مقابلة زخم تلك المبادرة فتتطلب ما هو أكثر من تجاهلها أو معارضتها، وعلى الولايات المتحدة، أن تتعدى حدود وظائف شركة الإنترنت للأسماء والأرقام المخصصة، بحيث تعمل بروح من التعاون، مع دول أخرى؛ بغية استحداث آلية مثلى؛ للتنسيق الدولي؛ لمكافحة الجريمة الإلكترونية، ووضع قواعد الحرب في الفضاء الإلكتروني، والترويج لتطوير تشكيلة جديدة آمنة، من بروتوكولات الإنترنت.

إعادة النظر في المصالح الأمريكية في الفضاء الإلكتروني

إن المصلحة القومية الطاغية للولايات المتحدة، في الفضاء الإلكتروني، تكمن في المحافظة على الإنترنت، وتوسيع نطاقها؛ بوصفها أداةً من أدوات الكفاءة الاقتصادية، داخل الوطن، وعاملاً ميسِّراً للتبادل الاقتصادي على المستوى الدولي، أما المستوى الحالي للنشاط الإجرامي والتجسس وإعداد ساحة المعركة في الفضاء الإلكتروني، فيهدد بتعطيل المكاسب الاقتصادية المتأتية من التوصيل الشبكي للنظم، طوال العقدين الماضيين، إن لم يكن يمحو تلك المكاسب كلها، وعلاوة على ذلك، فإن المبالغة في الاستجابة لتلك التهديدات، قد تكون لها الآثار المدمرة ذاتها، وعلى الولايات المتحدة - لدى سعيها لتحسين الأمن في الفضاء الإلكتروني - أن تعمل؛ للمحافظة على ما للشبكة من خصائص أساسية، ترفع إلى حد كبير، من قيمتها بالنسبة إلى التبادل الاقتصادي؛ أي: الابتكار والانفتاح والحوكمة المحدودة، وهذه الخصائص تجعل الشبكة مرنة، بحيث يسهل تطوير الاستخدامات الجديدة، وقابلة للتطوير، بحيث يمكن توصيل ملايين المستخدمين والأجهزة، كل عام؛ فيوسِّع ذلك نطاقي التدفق الحر للأفكار، والتجارة الدولية، لكن معالجة مشكلات الأمن في الفضاء الإلكتروني، على حساب تلك الخصائص، لن تخدم المصالح القومية الأمريكية.

إن المكاسب الهائلة - على صعيد الإنتاجية الاقتصادية - طوال العقدين الفائتين؛ هي نتيجة للاستخدام المباشر الموسَّع للإنترنت، في: الاتصال والتعاون والتعهيد وإدارة المخزون في الوقت المناسب؛ [على أساس تقليل الفاقد]، ومراقبة العمليات الصناعية، وعلى الصعيد الدولي، نجد أن ما حدث من توسّع في التجارة العالمية، في السلع والخدمات معاً، لم يكن ليتحقق لولا الإنترنت؛ بوصفها تكنولوجيا ممكِّنة، والنشاط الخبيث في الفضاء الإلكتروني، يهدد تلك النظم؛ ففي مجال التجسس بين الشركات وحده، بدأ الكثير من هذه الشركات، يشكك في الحكمة من استخدام الإنترنت؛ للسماح بالاضطلاع بنشاطات البحث والتطوير، على مدار الساعة، وفي جميع المناطق الزمنية؛ بسبب فقدان حقوق الملكية الفكرية؛ نتيجة للهجمات.

والولايات المتحدة؛ بوصفها البلد صاحب الاتصال الشبكي الأوسع نطاقاً في العالم، هي – أيضاً – البلد الأكثر عرضة للنشاط التخريبي في الفضاء الإلكتروني، سواء أكان ذلك النشاط، في شكل تهديدات للنظام ذاته، أو كان تهديدات موجهة عبر النظام، إلى أهداف موصَّلة شبكياً، وعلى الرغم من مكامن الضعف تلك، فإن إدارة أوباما، ماضية في خطط من شأنها الزيادة – لا التقليص – في اعتماد الولايات المتحدة، على التكنولوجيات الموصَّلة شبكياً؛ لتنفيذ تعاملاتها التجارية، ومراقبة النظم الحسّاسة، والاضطلاع بمسؤوليات الحكم، وتحدِّد "الخطة الوطنية للنطاق العريض"، الوصول الموسَّع للنطاق العريض؛ بوصفه «أساس تحقيق النمو الاقتصادي، وإيجاد الوظائف، وبلوغ التنافسية العالمية، والارتقاء بسبل الحياة»،[9] وتحدد الخطة ستة «أهداف؛ للوصول إلى أمريكا عالية الأداء»، تتيح من خلالها نظم الإنترنت، مكاسب كبيرة جديدة، على صعيد الكفاءة، في كل قطاع من القطاعات الاقتصادية، وفي الحياة اليومية لكل مواطن أمريكي، من دون استثناء، وتشمل الأهداف: إرساء شبكة وطنية للنطاق الواسع للمستجيبين الأوائل first responders؛ لتوفير الاتصال المتبادل في أوقات الكوارث، وشبكة "ذكية"، تصل أفراد المستهلكين بشبكة الكهرباء؛ لرصد استخدام الطاقة، ومعدله في الزمن الحقيقي؛ وبالنظر إلى بيئة التهديد الإلكتروني الحالية، نجد أن توسيع نطاق اعتماد الولايات المتحدة، ينطوي على سذاجة كبرى، ووضع أسوأ تصبح فيه الولايات المتحدة، عرضة لتهديدات أطراف حكوميين وغير حكوميين، يسعون لتجاوز ساحة المعركة، وإيذاء المجتمع الأمريكي، في الفضاء الإلكتروني.

وعلى الولايات المتحدة – لدى سعيها لتقليص تلك التهديدات – أن تراعي أيضاً، أن الأمن ليس هدفاً في حد ذاته، وإنما هو عامل ميسِّر للتبادلات التجارية، والارتقاء بالكفاءة؛ فالأمن المفرط، من شأنه: تقليص قابلية استخدام الشبكة، وإبطاء الحركة، وإقامة الحواجز، أمام الاستخدامات الجديدة والمستخدمين الجدد، وبينما توجد ضرورة لتقوية الحوكمة، فإن من الضروري كذلك، تكييف تلك الحوكمة، بحيث تعالج مجموعة محددة من الهواجس الأمنية التي ترتبط بالجريمة والحرب، والاقتراحات المقدمة من أطراف؛ كالصين وروسيا وأنظمة سلطوية أخرى؛ لتحسين "أمن المعلومات" – وهو التعبير الذي اختارته لذلك – لا تخصّ في الواقع، تلك الهواجس، وإنما ترتبط برغبة أولئك الأطراف في الحدّ من المعارضة، ومن الوصول إلى

المعلومات التي يُرى فيها تهديد لأنظمتها؛ فالاقتراحات بإدخال سبل تعقُّب لجميع الطرود: [أجزاء المعطيات الرقمية packet]، يمكن بمقتضاها على الفور، تعقُّب كل إجراء، يُتّخذ على الشبكة؛ وصولاً إلى فرد على سبيل المثال، من شأنها: إبطاء حركة الإنترنت، ورفع تكلفتها، من دون جني فائدة تُذكر، على صعيد مكافحة الجريمة، أو الحدّ من الحروب، بيد أن تلك الاقتراحات، ستسهم في تضييق قدرة المستخدم العادي، على الوصول إلى المعلومات، والدخول في الحوارات السياسية، من دون أن يُكشَف اسمه، وستجد الجماعات الإجرامية والأجهزة الاستخبارية والجيوش، سبلاً للالتفاف على تلك الضوابط، بينما سيخضع نشاط المستخدم العادي على الإنترنت، لمراقبة تكاد تكون كاملة،[10] ونظام كهذا، سيكون له تأثير خانق في إمكانية استخدام الشبكة، وسيلحق الضرر بالمصالح الأمريكية الممثلة بالترويج للحرية والديمقراطية حول العالم، وعلى الرغم من أنه لا يوجد الكثير مما يمكن الولايات المتحدة عمله؛ لإقناع لاعبين؛ كالصين وروسيا وأنظمة سلطوية أخرى، بأن في الوصول غير المقيَّد للإنترنت، وما يصاحبه من انفتاح وحرية تعبير، خدمة لمصالحها القومية، فإن المجتمع الدولي سيصيبه الضرر؛ إذا طُوِّرت الإنترنت العالمية، في الاتجاه الذي يجسد قيم تلك المجتمعات.

ولتفادي هذه النتيجة، والمحافظة - في الوقت ذاته - على الإنترنت، وتوسيع نطاقها؛ بوصفها أداةً للتبادل والكفاءة الاقتصاديين، فإن على الولايات المتحدة، أن تعمل ضمن المنظومة الدولية؛ لكبح الأطراف الفاعلين ذوي النيات الخبيثة، ووضع القواعد المضادة لاستهلال الصراعات في الفضاء الإلكتروني، أما البدائل لهذا النهج، فغير جذابة، وهي تشمل: الاضطرار إلى تقليص التوصيل الشبكي للنظم، وتوسيع نطاق الرقابة للأغراض الأمنية، على رغم تكلفته وصعوبته، والحماية الفعلية للبنى الأساسية الحيوية، في الفضاء الإلكتروني من الأجهزة الحكومية، على غرار الاضطلاع بأمن الشركات الجوية، في أعقاب الحادي عشر من أيلول/ سبتمبر، والتوسع في استخدام القدرات الهجومية؛ لوقف الهجمات؛ وإذا امتنعت الولايات المتحدة عن المشاركة، فإن دولاً أخرى، ستشكل مستقبل الإنترنت، ولكنها ستقوّض الشبكة؛ بوصفها آليةً للتبادل الحر للمعلومات وللتخاطب السياسي، ومن الواضح - في ضوء تلك البدائل - أن الحل المفضل، هو المشاركة الدولية؛ لتحسين أمن الفضاء الإلكتروني، وتحديد الحركة فيه.

مبادئ المشاركة

لم تَعُد الولايات المتحدة الأمريكية طرفاً لا غنى عنه، إزاء ما يتعلق بحوكمة الإنترنت، وامتناعها عن المشاركة في منتديات حوكمة الإنترنت، لن يمنع دولاً أخرى، ذات أهداف تتناقض وأهداف الولايات المتحدة، من تشكيل مستقبل الإنترنت، ولن تنال الولايات المتحدة شيئاً، من الظهور بمظهر المصمِّم على استخدام هجمات الشبكات الحاسوبية من دون قيود، وفي الوقت الذي يتعين فيه على الولايات المتحدة، أن تركز معظم جهودها، على بناء توافق آراء غير رسمي، واستحداث الآليات الدولية للتعاون، فإنها تكون بحاجة إلى أن تشارك؛ وفق شروطها هي، بدلاً من السعي لمنع المناقشة الدولية للموضوع؛ والحديث لن يعود عليها بخسارة تُذكر.

وعلى الولايات المتحدة - من حيث المبدأ العام - أن تدعم العمليات التي تسمح لممثلين من المجتمع التقني، والقطاع الخاص، وأوساط المستخدمين والمستهلكين، أن يشكِّلوا السياسات، وتفادي العمليات التي تكون الدولة مركزها؛ لمعالجة المسائل التقنية، بيد أن المنظمات الحكومية الدولية ضرورية؛ لخضوع الإنترنت لسيادة القانون، ومن خلال المشاركة، تستطيع الولايات المتحدة أن تضع الحلول للتحديات الأمنية، في الفضاء الإلكتروني، على نحو يتفق والمصالح الأخرى المتأتية من اتساع نطاق التجارة الدولية، وتحقيق المزيد من الكفاءة الاقتصادية، وسيتعين على الولايات المتحدة، أن تضع أجندات منفصلة، واستراتيجيات؛ لتحقيق تلك الأجندات، في مجالات الجريمة، والحدّ من دور الدول، واستحداث المعايير الآمنة، ولكنْ، ثمة مجموعة من المبادئ الشاملة التي ينبغي أن توجِّه المشاركة الأمريكية عموماً، في هذا المجال.

اعتماد "نهج شبكي وموزّع"

على الولايات المتحدة - لدى سعيها لتحقيق مصالحها الوطنية في الفضاء الإلكتروني - أن تدعم العمليات المفتوحة التي ترحِّب بطائفة واسعة من المشاركين، من: الوسط التقني، والقطاع الخاص، وجماعات المستخدمين والمستهلكين؛

لتشكيل السياسات، وتجنُّب العمليات التي تكون الدول مركزها؛ لمعالجة المسائل التقنية؛ ذلك أنه ما من منتدى، يمكنه - وحده - أن يشمل جميع القضايا واللاعبين المعنيين بتبديد الهواجس الأمنية، في الفضاء الإلكتروني، وعلى الولايات المتحدة - بدلاً من ذلك - أن ترعى طائفة من المنتديات - بعضها متعدد الأطراف، وبعضها ثنائي، وبعضها إقليمي - للتصدي لتلك التحديات، وقد يلزم إنشاء ائتلافات منفصلة؛ لمعالجة الأجندة التقنية، والجوانب المختلفة من الأجندة القانونية الدولية؛ ومن ذلك: الجريمة، وتجسس الشركات، والصراعات بين الدول، وتستطيع الائتلافات الإقليمية، أن تثبت فعاليتها أيضاً؛ فعلى الرغم من أن التهديدات الإلكترونية، لا تتباين كثيراً من إقليم إلى آخر، فإن بلوغ سلسلة من الاتفاقات، ضمن المنظمات الإقليمية، قد يكون أسهل من بلوغ اتفاق عالمي، وبدلاً من السعي لاستمالة المستعمرات القديمة؛ للدخول في معاهدات، وضعتها قوى استعمارية سابقة، فإن اعتماد محاكاة اتفاقية مجلس أوربا الخاصة بالجرائم الإلكترونية، في إطار منظمة الدول الأمريكية، والاتحاد الإفريقي، ورابطة أمم جنوب شرق آسيا (آسيان)، قد يكون أكثر تأثيراً، أما الائتلافات العالمية التي تعنى بأنماط مشكلات أكثر تحديداً، فهي - أيضاً - يمكنها أن تكون ذات تأثير؛ فبدايةً، يجب أن تكون تلك الائتلافات مرنة، وغير رسمية، وأن تسعى للحصول على دعم الدول التي تتفق مصالحها ومصالح الولايات المتحدة، أما حلفاء الولايات المتحدة التقليديون، فهم نقطة بداية حسنة، ولكنْ، لا بد من بذل الجهود؛ لاستقطاب ما يزيد على الحفنة التقليدية، من المشتبه بهم من الغربيين، ويمكن أن تشمل قائمة الدول التي سيُطلب دعمها: الدول الإحدى والثلاثين الأعضاء في منظمة التعاون الاقتصادي والتنمية، إلى جانب دول صغرى ودول ذات نمو أقل، وتسعى لمعالجة الجريمة الإلكترونية؛ ومنها: أستونيا والفلبين والجمهورية الدومينيكية.

مساءلة الدول على أفعالها

ظلّ خبراء الاستراتيجية الأمنية، مقيَّدي الحركة؛ بسبب "مشكلة الإسناد، [أو العزو]"، طوال أكثر من عقد، وإسناد الهجمات الإلكترونية؛ [أي تحديد الجهة المسؤولة عنها]، أمر تصعِّبه عوامل أربعة: العامل الأول هو أن الهجمات الإلكترونية، لا تتطلب

قرباً جغرافياً، والثاني هو أنه لا يوجد معادل لنظم الرادار؛ لكشف مصدر الهجوم؛ كما كانت عليه الحال بالنسبة إلى صواريخ الحرب الباردة، والثالث هو أن البروتوكولات التي تحكم حركة الإنترنت، تفتقر إلى الأمن أساساً، ومصدر الطرود يمكن حجبه، والرابع هو أن منفِّذي الهجمات الإلكترونية، يستخدمون - عادةً - نظاماً أو أكثر، من النظم المتضررة؛ بوصفها نقطةَ انطلاق لهجومهم، ويتخطّون الكثير من الحدود الدولية؛ لتعقيد عملية التحرّي.

وبينما توجد ضرورة للسعي لحلّ مشكلة الإسناد، والمشكلات الأمنية الأخرى المرتبطة ببنية الإنترنت، فإن من الضروري، عدم تضخيم مشكلة الإسناد؛ ففي المرحلة الحالية، تُحصر القدرة على شنّ أي شيء يرتقي إلى مستوى "الحرب"، في الفضاء الإلكتروني، في عشرين جماعة على الأكثر، على المستوى العالمي: نصفها من الجهات الحكومية، بينما النصف الآخر جماعات إجرامية خاصة، وهي وثيقة الصلة بدول، وفي حال حدوث هجوم كبير الحجم، فإن قائمة المشتبه بهم، ستكون قصيرة، ومازال السبل التقنية؛ للتعرف إلى منفِّذي الهجمات تشهد تحسناً، ولكنْ، لا بد من عدم إغفال أهمية الاستخبارات والتحقيقات، في العالم الحقيقي، وربما لا يتاح الإسناد اليقيني بالوسائل التقنية على الإطلاق؛ نظراً إلى أن المجرمين والمحاربين الإلكترونيين، سيعملون على استبانة مواضع الضعف، في أي نوع من البروتوكولات، أو نظم مراقبة جديدة، وإن أمكن - على الدوام تقريباً - التوصل إلى ما يشبه السبب المحتمل؛ لإجراء المزيد من التحقيقات.

وعندما تحدث الهجمات الإلكترونية، سوف نجد - في الكثير من الحالات - نفي الدول مسؤوليتها، وإشارة إلى "متسللين، [أو قراصنة] وطنيين"، لا يمكن التعرف إلى هويتهم، أو السيطرة عليهم؛ بوصفهم الجناة المحتملين، كما ترفض الدول، السماح للمحققين، بالوصول إلى المشتبه بهم المحتملين، أو إلى النظم المرتبطة بالحدث؛ لأن ذلك من شأنه: الإخلال بالسيادة الوطنية، وفي مناسبتين على الأقل - ونقصد: مسألة الهجومين على أستونيا وجورجيا - كان ذلك هو الرد الروسي، وبصورة مماثلة، تنفي الحكومة الصينية أي مسؤولية عن الهجمات الإلكترونية التي تنشأ من "أنظمة" كائنة في أراضيها،

وفي أوائل عام 2010، تمكنت شركة جوجل، من تعقّب حملة تسلُّل ناجحة، تم خلالها سرقة معلومات مملوكة؛ [أي سرقة أسرار تجارية]، من جوجل، وشركات أمريكية، بلغ عددها: ثلاثين شركة؛ وصولاً إلى خادمات servers، في الصين، وقد جادل مسؤولون في الحكومة الصينية بأن النظم المستخدمة في الهجمات، هي نظم وكيلة، تم النيل منها؛ بسبب اتساع نطاق استخدام البرامج المقرصنة، والنظم غير الآمنة في بلدهم، وقد يكون هذان التفسيران صحيحين، ولكنْ، في كلا المثالين، وفي ظل وجود أدلّة تشير إلى نشاط إجرامي؛ يستهدف بلداً، ويمكن تعقُّبه؛ وصولاً إلى بلد آخر، فإن عبء الإثبات، يجب أن ينتقل الآن إلى البلد الذي يستضيف النشاط غير المشروع، وعلى الدول التي لا تتعاون في التحقيقات الجنائية، أن تفهم أن عدم التعاون، سيُفسّر على أنه علامة على التواطؤ، ويمكن أن تُحاسَب الدول على أفعالها، وعلى أفعال مواطنيها، وعلى النظم في الفضاء الإلكتروني،[11] وتتطلب الولايات المتحدة، طائفة من الخيارات والآليات؛ لمعاقبة الدول التي تهاجم دولاً أخرى في الفضاء الإلكتروني، بصفة دورية، أو تسمح بأن تُستخدم أراضيها أو نظمها من جماعات إجرامية، وأما الاستجابات فيمكنها أن تشمل الأسلوب التقليدي، وهو الممثل بالاحتجاجات الدبلوماسية، والعقوبات، والعمل العسكري، و - كذلك - التدابير الشبكية؛ ومنها: الارتقاء بمستوى مراقبة حركة الإنترنت الخارجة من الدول غير المتعاونة، وانتهاءً بمنع الدول التي تواصل التغريد خارج السرب، من الوصول إلى شبكات الولايات المتحدة وحلفائها.

القيادة بالقدوة

لا تستطيع الولايات المتحدة أن تدعو الآخرين إلى التحرك، من دون أن تلتزم أيضاً، بضبط النفس، في استخدام القوة في الفضاء الإلكتروني، وكبح مرتكبي الجرائم الإلكترونية في الداخل، واتخاذ الخطوات اللازمة؛ للحد من النشاط الخبيث، في الشبكات الأمريكية، ويجب أن تُبرِز الجهود الدبلوماسية الأمريكية - بوضوح - أن النشاط العسكري والنشاط الاستخباري الأمريكيين، في الفضاء الإلكتروني، إنما يركزان على الدفاع عن الولايات المتحدة، وحماية حرية تدفق المعلومات على المستوى الدولي، وعلى الولايات المتحدة أن تتشدد في التزام ملاحقة أي مواطن، يضلع في "القرصنة الإلكترونية لدوافع سياسية"، ضد

دول أجنبية، وأن تطالب الدول الأخرى، بالقيام بالـشـيء ذاتـه، وإزاء مـا يتعلـق بـالجرائم الإلكترونية، لا بد من توفير الأموال لمكتـب التحقيقـات الاتحـادي؛ كـي يخـصِّص مـوارد؛ للتحقيق في النشاط الإجرامي الإلكتروني المنطلق من الأراضي الأمريكية؛ ولكنـه يـستهدف ضحايا في الخارج، وعلى الولايات المتحدة، أن تقود – أيضاً – الجهود؛ لتنظيف حيِّزهـا مـن الفضاء الإلكتروني، من خلال: تقليص حصتها من الحواسيب الموصَّلة بالشبكة التي تكون: إما أجزاء من "بوتنتات" botnets – أي شبكات من الحواسيب المصابة التي تُـستخدم لـشنِّ الهجمات – أو تكـون نقـاطاً لاستـهلال الهجـمات، كـما أن عـلى الولايـات المتحـدة، أن تعمل – كذلك – على إرساء آليات؛ لإحباط الهجمات عـلى الـنظم الأجنبيـة، المنطلقـة مـن النظم الأمريكية، في الوقت الحقيقي.

السعي للمشاركة الدولية

على الولايات المتحدة أن تسعى؛ مسترشدة بمجموعة من المبادئ، لتحقيق مصالحها على مسارات ثلاثة؛ وهي: أولاً، أن تقود عملية إنشاء مجموعة من نظم دولية أقوى؛ لمكافحة الجريمة في الفضاء الإلكتروني؛ ومادامت المعالجة المنفردة للجريمة الإلكترونية - ثانياً - لن تفضي إلى تقليص التهديدات للشبكة، ولنظامها، بالمستوى الذي يكفي؛ كي تصبح الثقة بها ممكنة، فإن على الولايات المتحدة، أن تنتهج - كذلك - مساراً آخر؛ لتقييد الأطراف الحكوميين في الفضاء الإلكتروني، وأخيراً، على الولايات المتحدة، بذل الجهود؛ لتأمين التكنولوجيات الأساسية للإنترنت.

الحدّ من تهديد الجريمة الإلكترونية

أصبحت الجريمة الإلكترونية، مهنة المجرمين الأذكياء المفضلة؛ نظراً إلى أنها تنطوي على مخاطر محدودة، ومردود عالٍ، وبينما السلطة الوطنية المشروعة، تقيدها الحدود، فإن شبكة الإنترنت ليست كذلك، ويستغل المجرمون هذه الحقيقة، بارتكاب الجريمة الإلكترونية في أحد البلدان؛ انطلاقاً من الحدود الآمنة لبلد آخر، يُفضل أن يتسم بضعف قوانينه، ومحدودية قدراته على إنفاذ القوانين، أو إجراء التحقيقات، أو ملاحقة الجناة؛ ومن هنا، فإن مكافحة الجريمة الإلكترونية، تقتضي أن تسنّ الدول أي قوانين، تعاقب على الجريمة الإلكترونية الدولية، وترسي آليات؛ لوقف الهجمات الناشئة، في أحد البلدان؛ لاستهداف ضحايا في بلد آخر، والتحقيق في تلك الهجمات، وملاحقة مرتكبيها، وتوجد حاجة إلى أن تلقي الولايات المتحدة ثقلها، وراء المبادرات المتعددة الأطراف التي تساعد الدول على تطوير أطرها القانونية، وتعزيز قدراتها، وإرساء آلية لتقويم مدى فعالية الجهود الوطنية؛ لمكافحة الجريمة الإلكترونية، وتنفيذ عملية، تشتمل على حوافز إيجابية وسلبية: [أي عقوبات] تروِّج للتقيد بالمعايير القانونية الدولية.

تركيز الجهود خارج نطاق اتفاقية مجلس أوربا حول الجريمة الإلكترونية

رُكِّزت الجهود الرامية إلى بلورة حلٍ لمشكلة الجريمة الإلكترونية الدولية، في اتفاقية مجلس أوربا حول الجريمة الإلكترونية، وقد صيغت الاتفاقية؛ لتحديد مجموعة أساسية من القوانين التي يتعين على الأطراف في الاتفاقية اعتمادها؛ لتجريم جرائم الحاسوب، وتوفير آلية للتعاون العابر للحدود،[12] وألقت الولايات المتحدة ثقلها، خلف اتفاقية عام 2000، بعد أن تعثرت محاولة محاكمة منشئ الفيروس الحاسوبي المعروف باسم "آي لاف يو" ILOVEYOU؛ ففي تلك الحادثة، تمكنت سلطات تنفيذ القانون، في الولايات المتحدة، من تعقُّب منشئي الفيروس، وهم مجموعة من الطلاب في الفلبين، ولكنها لم تفلح في إقناع السلطات الفلبينية، بتسليم منشئ الفيروس؛ نظراً إلى أن الجريمة التي ارتكبها غير مخالفة لقانون الفلبين، وقد وُضعت الاتفاقية في شكلها النهائي، في تشرين الثاني/ نوفمبر عام 2001، ودخلت حيز التنفيذ في تموز/ يوليو عام 2004، بعد أن صدّقتها دول خمس، وفي أيار/ مايو عام 2010، كان قد صدقها تسعة وعشرون بلداً، بينما كان ينظر في عملية التصديق، سبعة عشر بلداً.[13]

وبينما ساعدت الاتفاقية، على إرساء معيار دولي؛ لتجريم الجريمة الإلكترونية، فإنها لم تؤدِّ إلى تراجع ملحوظ في معدلات تلك الجريمة؛ ذلك أن آليات التعاون الدولي التي استحدثتها الاتفاقية، ثنائية، وتتعلق بالملاحقة القضائية، ولا تفسح المجال؛ لتنسيق نشاطات تنفيذ القانون، عبر الحدود، أو لقيام المهنيين في مجال أمن الشبكة، بتنسيق الحلول التقنية لدى وقوع الهجمات، ويضمّ أعضاء الاتفاقية، بعض أسوأ ملاذات مرتكبي الجرائم الإلكترونية في أوربا الشرقية؛ مثل: رومانيا وبلغاريا، وهناك الكثير من الدول – وخاصة اليابان – لم تكن راغبة في تصديق المعاهدة؛ لأنها اشتُرعت في إطار مجلس أوربا فحسب، وقد أسهمت الاتفاقية في إرساء الإطار القانوني؛ لمواءمة القوانين الوطنية بشأن الجريمة الإلكترونية، وتقديم المساعدة المتبادلة عبر الحدود، بيد أن زيادة عدد الأطراف الموقِّعين على هذه الوثيقة، بصورة خاصة، ليست ضرورية ولا كافية؛ للحد من نشاط الجريمة الإلكترونية العابرة للحدود؛ وخلافاً لمعاهدات الحدّ من التسلح؛ حيث لا يمكن أن تقوم دولة بتخفيض قواتها، إلا بعد اتفاق الأطراف كافة، على تخفيض

للقوات، فإن اعتماد القوانين المتعلقة بالجريمة الإلكترونية، يصبّ في مصلحة دول منفردة، بصرف النظر عن احتمال كون الدول الأخرى، قد اعتمدت تلك القوانين، أوْ لا؛ لأن مجرمي الإنترنت، يميلون إلى عدم قصر نشاطاتهم، على الأهداف الأجنبية.

استخدام فرقة العمل المعنية بالعمل المالي نموذجاً

على الرغم من أن على الولايات المتحدة، أن تدعم، عامةً، العمليات البعيدة عن المركزية، والجامعة للمجتمع التقني، والقطاع الخاص، وجماعات المستخدمين والمستهلكين، فإن هناك مشكلات، لا يمكن معالجتها إلا من خلال الدول، والجريمة الإلكترونية إحدى تلك المشكلات، ولدى استحداث نظام جديد؛ للحدّ من الجريمة الإلكترونية على المستوى الدولي، فإن الهدف يجب أن يكمن في أن تتم معالجة المشكلات القائمة على صعيد التحقيق مع مرتكبي الجرائم الإلكترونية وتوقيفهم وملاحقتهم قضائياً، على نطاق ضيق، وبأقل قدر ممكن من التنظيم، وفي المجالات التي تكون الحكومات وحدها، هي من يقوم بمعالجة مشكلات الفضاء الإلكتروني، فإن عليها أن تقوم بذلك، في أضيق الحدود الممكنة.

كما أن على الولايات المتحدة، أن تروِّج اعتماد القوانين الجنائية، على المستوى الوطني، واستحداث آليات ذات طابع رسمي أخفّ، إزاء ما يتعلق بالتحقيق، والملاحقة القانونية عبر الحدود، من خلال إنشاء جهاز حكومي دولي جديد، يتم تصميمه؛ وفق فرقة العمل المعنية بالعمل المالي، وهي منظمة، أنشئت للترويج لوضع السياسات، وتطوير القدرات الوطنية والدولية؛ لمكافحة تمويل الإرهاب وغسل الأموال،[14] وقد استهلت فرقة العمل - وهي التي أسستها عام 1989، مجموعة البلدان السبعة، بالتنسيق والمفوضية الأوربية، وثمانية بلدان أخرى - عملها، بوضع مجموعة من أربعين سياسة، توصي الدول باعتمادها؛ وسرعان ما اتسع نطاق فرقة العمل، بحيث أصبحت الآن، تضمّ أربعاً وثلاثين دولة، تمثل مجتمعةً معظم المعاملات المالية العالمية، وفي أعقاب الهجمات الإرهابية في الحادي عشر من أيلول/ سبتمبر عام 2001، أضيفت مهمة مكافحة تمويل الإرهاب، إلى مهمات فرقة العمل، وروجعت معاييرها؛ لمعالجة المسألة الجديدة، وإلى

جانب وضع السياسات والمعايير الموصى بها، فإن فرقة العمل، ترصد مدى امتثال الأعضاء لتلك المعايير، وتساعد على تنفيذها، وتتم عملية الرصد؛ على أساس استعراض أقران متعددي الأطراف، في إطار برنامج، يُعرف باسم "التقويم المتبادل"، كما تمخضت فرقة العمل، عن سلسلة من الأجهزة الإقليمية، على الطراز نفسه، تضطلع بمهمات مماثلة، ضمن مناطق جغرافية محددة،[15] ولدى فرقة العمل، طائفة متفق عليها، من المعايير والآليات المحددة؛ لرصد الامتثال، وهي تشكل الأساس الذي تستطيع الولايات المتحدة، ودول أخرى، أن تستند إليه، في تهديد الدول غير الممتثلة، بالحرمان من سبل الدخول إلى الشبكات المالية الدولية.

ولا بد من إنشاء منظمة شبيهة، تقوم، إزاء ما يتعلق بالجريمة الإلكترونية، بما تقوم به فرقة العمل المعنية بالعمل المالي، على صعيد غسل الأموال، وعلى الولايات المتحدة أن تنشئ هذه المنظمة، بالتعاون بينها وبين الدول الأخرى الأعضاء في منظمة التعاون الاقتصادي والتنمية، والدول الأصغر حجماً المؤيدة لجدول أعمال المنظمة، وأن تضع معايير تقويم طلبات العضوية التي تتقدم بها الدول الأخرى، ولا بد أن تبدأ المنظمة، بوضع سياسات نموذجية، تستند إلى اتفاقية مجلس أوربا، ومجموعة أدوات الاتحاد الدولي للاتصالات، بشأن تشريعات الجريمة الإلكترونية، وممارسات مثلى أخرى معترف بها؛[16] وكما هي الحال بالنسبة إلى فرقة العمل المعنية بالعمل المالي، لا بد أن يكتمل العمل، خلال العام الأول من إنشاء المنظمة؛ وإثر وضع السياسات الموصى بها، يجب أن تشرع المنظمة، في تقويم البلدان الأعضاء، من حيث المعايير الموضوعة، كما ينبغي أن توفِّر عمليات التقويم، خطة لتصحيح أي مشكلات يتم التعرف إليها، وأن ترسي عملية للاستعراض الدوري، إزاء التقدم المحرز في معالجة تلك المشكلات.

تسمية ملاذات مرتكبي الجريمة الإلكترونية وفضحها ومعاقبتها

على المنظمة كذلك، أن تجري استعراضاً عالمياً سنوياً، للدول الأعضاء وغير الأعضاء معاً؛ لتقويم الأطر القانونية والقدرات، على تنفيذ القانون والمستويات الشاملة للجريمة الإلكترونية لدى الدول، وأما ما يخصّ المشكلات عبر الوطنية الأخرى، فإن إعداد مؤشر

أو تقرير سنويين، بشأن البلدان الأفضل والأسوأ؛ انطلاقاً من قياسات موضوعية، دعا دولاً كثيرة إلى تحسين سلوكها، وتشمل النماذج، مؤشر الفساد الذي تعدّه منظمة الشفافية الدولية، والتقرير العالمي، حول المخدرات، وهو الذي يعدّه مكتب الأمم المتحدة المعني بالمخدرات والجريمة، ومؤشر شؤون الحوكمة، وهو الذي يعدّه البنك الدولي، وقد شرع منتدى رسم خرائط الجريمة الإلكترونية وقياسها، وهو التابع لمعهد أوكسفورد للإنترنت، في استكشاف القياسات الممكن استخدامها، في مثل ذلك التصنيف،[17] وتلك التصنيفات، ستكون آلية فعّالة؛ لـ "التسمية والفضح" للدول؛ حتى تتصدى لنشاطات الجريمة الإلكترونية، وتنضم إلى عضوية المنظمة الجديدة.

ويمكن – عندئذٍ – استخدام تلك التصنيفات المستقلة؛ أساساً تعمل المنظمة وفقه، مع البلدان الأسوأ؛ لوضع خطط سدّ الفجوات في آلياتها الخاصة بالشؤون القانونية وتنفيذ القانون؛ وفي نهاية المطاف – كما هي الحال بالنسبة إلى توصيات فرقة العمل المعنية بالعمل المالي وتقويماتها – يمكن أن توفّر تلك العملية، الأساس الذي يتم الاستناد إليه، في معاقبة الدول؛ لعدم تصديها لنشاط الجريمة الإلكترونية، ويمكن فرض العقوبات؛ على أساس ثنائي أو أساس متعدد الأطراف، ويمكنها أن تشمل منع المعونات المالية الإنمائية الهادفة إلى تطوير البنى الأساسية للإنترنت، أما الدول التي لا تنظّف حركة المرور الدولية للإنترنت لديها، فيمكنها أن تخضع لـ "فحص المحتوى العميق"،* أو مستويات مرتفعة أخرى من المراقبة؛ بما يبطئ تدفق حركة المرور [لديها]، كما أن عدم تحقيق تحسّن، يمكن أن يؤدي – بوصفه ملاذاً أخيراً – إلى أن تقوم الدول الأعضاء في المنظمة، بوضع طوائف من بروتوكولات الإنترنت الوطنية الخاصة بالدول الأكثر انتهاكاً على القائمة السوداء.[18]

ربط مساعدات تطوير البنى الأساسية للإنترنت بالتعاون في مجال الجريمة الإلكترونية

على المنظمة الجديدة أن تعمل أيضاً، مع المنظمات الدولية التي تروّج لتطوير البنى الأساسية للإنترنت؛ لضمان أن تنفّذ تلك الاستثمارات، مقترنةً بالاستثمارات في تطوير القدرات، إزاء ما يتعلق بالجوانب القانونية والتصدي للحوادث وإنفاذ القانون، وهذا

---

* أو عملية التحليل العميق للحُزَم؛ أي قيام مزود خدمة الإنترنت، بتتبع البيانات التي تمر عبر الشبكة. (المترجم)

الجهد يمكن الترويج له داخل الحكومة الأمريكية أيضاً؛ فالمشروعات التي تضطلع بها وكالة التنمية الدولية التابعة للولايات المتحدة؛ لمدّ شبكات كابلات الألياف البصرية في البلدان النامية، يجب أن تتم بالتنسيق بينها وبين المساعدة القانونية المقدمة من وزارة العدل؛ لتطوير القدرات في مجال التحقيقات والملاحقة القضائية، وفي الوقت الحالي، لا يوجد رابط بين الجهدين، وعلى وزارة الخارجية الأمريكية، أن تضغط على الدول الحليفة والمنظمات الإنمائية الدولية؛ لاعتماد سياسات مماثلة.

إنشاء مراكز عمليات لتنسيق طلبات المساعدة

يمكن أن تساعد المنظمة، أخيراً، على حلّ مشكلة التنسيق الدولي؛ لوقف الجرائم الإلكترونية المستمرة، والتحقيق في الهجمات التي تعبر الحدود الدولية، إثر وقوعها وملاحقة مرتكبيها، والعملية الثنائية الحالية بطيئة ومضنية وعالية التكلفة، حتى بالنسبة إلى الولايات المتحدة، بسفاراتها التي لا ينقصها الموظفون وملحقاتها القانونية، وهي المنتشرة في مختلف أنحاء العالم، فضلاً عن الدول الصغيرة التي كثيراً ما تقع ضحية للجريمة الإلكترونية، وقد وضعت المجموعة الفرعية حول جرائم التقنية العالية التابعة لمجموعة البلدان الثمانية، أسس ذلك الجهد، من خلال إرساء آلية للتعاون، بشأن الجريمة الإلكترونية، تعمل على مدار الساعة طوال أيام الأسبوع، وهذا الجهد يمكن تحسينه من خلال جعل المنظمة تنشئ مراكز عمليات في جميع أنحاء العالم، يعمل فيها موظفون في مجال تنفيذ القانون من الدول الأعضاء، ويمكن تلك المراكز أن توفِّر موارد متاحة بصورة مستمرة، ورابطاً قيّماً بين موظفي تنفيذ القانون، ومراكز عمليات أمن الشبكة، وينبغي أن يكون من بين أهداف ذلك الجهد، استحداث آلية، يتم من خلالها، إرسال الطلبات التي ترد من الوكالات الحكومية والقطاع الخاص، في إحدى الدول، إلى السلطات في دولة أخرى؛ ومن ثمّ تمريرها إلى مشغّلي الشبكة؛ لإغلاق مزوِّدي خدمة القيادة والتحكم، أو مضيفي البوتنتات.

الحدّ من العمل الحكومي في الجريمة الإلكترونية

إن الجريمة الإلكترونية، ما هي إلا جزء من النقص الأمني الحالي في الفضاء الإلكتروني، وقد يكون في النشاط الحكومي، تقويض للثقة في الشبكة، أكثر مما يكون في

نشاط مرتكبي الجريمة الإلكترونية، وبينما يمكن التهوين من الجريمة الإلكترونية؛ بوصفها تكلفة للقيام بالأعمال، فإن أعمال الأطراف الحكوميين، تهدد نموذج الموصولية ذاته، وما يتبعه من مكاسب، على صعيد الكفاءة؛ ولأن الأطراف الحكوميين لديهم قدرات عالية عموماً، فإنه ما من شيء موصول بالشبكة، يعد بعيداً عن متناول يدهم؛ ولذا، فلا بد من كبحها بوسائل أخرى؛ إذا صعب كبح الدول بواسطة الدفاعات التقنية، وإذا لم يمكن فرض القيود، فقد تؤدي مكاسب الكفاءة المتأتية من الاتصال بالشبكة، إلى تحمّل تكلفة تفُوق قيمتها، وإذا تواصل الاستغلال الروتيني للبنى الأساسية الحساسة، فإن إعداد ميدان المعركة ذاته، قد يؤدي إلى نشوب صراعات لم تكن لتنشب، وإذا استمرت الدول في استهداف الملكية الفكرية للشركات الأجنبية، ونقل تلك الملكية إلى الشركات الوطنية، فإن ذلك قد يؤدي إلى تفكُّك النظام العالمي للبحث والتطوير، وهو الذي يتيح تنفيذ العمل على مدار الساعة.

إنهاء الاعتراض على المحادثات بشأن الحرب والتجسس في الفضاء الإلكتروني

لمعالجة تلك الهواجس، على الولايات المتحدة أن تعمل على وضع قواعد جديدة لسلوك الدول في الفضاء الإلكتروني؛ فطوال العقد الفائت، كانت الولايات المتحدة تتخذ موقفاً معارضاً لأي مناقشات حول هذه المجالات، وكانت تسعى لحصر تركيز المجتمع الدولي على معالجة الجريمة الإلكترونية، والاعتراض الأمريكي نابع من رؤية؛ مفادها: أن الدول لن تحترم التزاماتها بتقييد نشاطاتها في الفضاء الإلكتروني، وأن التحقق من وفاء الدول بالتزاماتها، سيكون أمراً شبه مستحيل،[19] بيد أن هذا الموقف نابع من تطبيق تجربة الحدّ من التسلح إبّان الحرب الباردة، وهو أمر لا يسهل تطبيقه على مشكلة أمن الفضاء الإلكتروني الحالية؛ فالاتفاقات الدولية المحدودة والمركزة، يمكنها أن تفيد الولايات المتحدة في بعض الحالات، وعلاوة على ذلك، فإن عدم رغبة الولايات المتحدة، في خوض مفاوضات حول هذا الموضوع، يزيد مصداقية الرأي الذي مفاده: أن الولايات المتحدة تسعى للسيطرة على الفضاء الإلكتروني.

والولايات المتحدة هي شبح الفضاء الإلكتروني الأكثر إثارة للخوف؛ بالنظر إلى دورها التاريخي في تطوير التكنولوجيات الأساسية، وارتفاع مستوى القدرات، ضمن: الجيش الأمريكي، وأجهزة الاستخبارات الأمريكية، أما المحافظة على تفوق القدرات الأمريكية – من حيث الاستغلال والهجوم مقارنة إلى المنافسين كافة – فأمر يخدم المصالح الأمريكية حقاً! ولكن، من المؤكد أن ما لا يخدم تلك المصالح، هو إدراك الآخرين أن الولايات المتحدة، تمتلك تلك القدرات وتستغلها، وأما عسكرة الفضاء الإلكتروني، فتشكل تهديداً على وحدة الشبكة وعالميتها وتبادليتها، وهذه العوامل كان لوجودها أثر كبير في: تحقيق النمو الاقتصادي الواسع النطاق، وتوثيق العلاقات بين الدول، من خلال التجارة المشتركة، وتسريع تبادل الأفكار عبر الحدود الثقافية والدولية، ولا يؤدي رفض المشاركة العلنية في مفاوضات حول الحدّ من الحرب الإلكترونية، إلا إلى زيادة المخاوف، بشأن كون الولايات المتحدة تسعى للسيطرة على الفضاء الإلكتروني، وتخطط لاستغلال النطاق؛ لنيل ميزات قتالية، وعلى الولايات المتحدة، أن تبذل ما في وسعها لمواجهة ذلك التصور، وبينما نجد أن المفاوضات ربما لا تفضي إلى إبرام اتفاقية، فإنها لن تسبب أيضاً، أي أضرار، وقد تبنَّت إدارة أوباما مبدأ الحوار على المستوى الدولي، ولا يجوز أن تُستثنى الحرب الإلكترونية من ذلك، وتعدّ مشاركة الولايات المتحدة في فريق الخبراء الحكوميين، وهو التابع للأمم المتحدة، بداية طيبة، ولكن التواصل يجب أن يكون أوسع وأعمق بكثير.

بيد أن التواصل لا يعني أن الولايات المتحدة مضطرة إلى قبول خيارات الاتفاقيات القائمة التي لا تصب في مصلحة الولايات المتحدة؛ فالاقتراح الروسي الحالي بشأن الحدّ من التسلح في الفضاء الإلكتروني، يُلزم الأطراف الموقِّعين بالامتناع عن تطوير قدرات إلكترونية هجومية، أو الضلوع في التجسس الإلكتروني، بينما يخلو من الآليات الناجعة للتحقُّق، وسجل اتفاقيات الأسلحة الكيميائية والبيولوجية، يثير الشكوك في شأن أن بالإمكان أن تفضي الالتزامات التي لا مجال للتحقق منها، إلى تقليص حقيقي، وعلاوة على ذلك، نجد – حال وفاء الولايات المتحدة بالتزاماتها، وتخلُّف الدول الموقِّعة الأخرى – أن اتفاقية من دون آلية تحقُّق؛ تعني أن الولايات المتحدة ستخسر ميزاتٍ استراتيجية.

والتركيز على تقييد تطوير الأسلحة الإلكترونية، ينمّ عن عدم فهـم للطبيعـة الحقيقـة للحرب الإلكترونية؛ فالتهديدات المتقدمة في الفـضاء الإلكـتروني، لا تكمـن في البوتـات bots،* أو الديدان worms،** وإنما في العنصر البشري، والسلاح الأقـوى لـيس القنابـل المنطقيـة،*** أو أحـصنة طـروادة،**** وإنـما البـشـر الـذين يـصممونها، ويمكـنهم استخدامها؛ بوصفها جـزءاً مـن مجهـود مـستمر مـنظم؛ للوصـول إلى الـنظم المـستهدفة، واستغلالها؛ سعياً لنيل الميزات المعلوماتية وإفساد البيانات أو تدميرها، وعلاوة على ذلك، فإن أي برنـامج دفـاعي، يتطلـب إتقـان العمليـات الهجوميـة؛ حتـى يمكـن صـدّ تلـك العمليـات، وفي الحـرب الإلكـترونية، نجـد أن القـدرة عـلى استنـساخ الـبرامج الحاسوبية؛ تعني – على الفور – أن أي خطوات يتم تطويرها؛ لأغـراض اختبـار التـدابير المضادة، يمكنها أن تتحول بسرعة إلى عملية هجومية، وفي ظـل هـذه الحقيقـة، لـن تحقـق محاولات الحدّ من تطوير العمليات الإلكترونية الهجومية النجاح؛ لأن التحقـق مـن كـون الدول لم تطوِّر مثل تلك القدرات، سيكون أقرب إلى المستحيل.

تفحُّص خيارات الاتفاقيات واستحداث القواعد في مواجهة استهداف النظم المدنية

إن وجـود مـشكلة التحقـق؛ لا يعنـي أنـه لا توجـد مـسائل، يمكـن المفاوضـات والاتفاقات الدولية، أن تعالجها على نحو مفيد؛ فبدلاً من التركيـز عـلى الحـدّ مـن تطـوير الأسلحة الإلكترونية، يجب على جهود الاتفاقيات، أن تركز على الحدّ من اختراق الجهـات الحكومية للنظم المدنية، ذات القيمة الاستخبارية المحـدودة أو ذات القيمـة الاسـتخبارية المعدومة، وفي المرحلة الراهنة، هناك الكثـير مـن الـدول التـي تـشنّ عمليـات إلكترونيـة هجومية، تحت غطاء منفصل، ولكنه ذو صـلة؛ ومفـاده: "التجـسس"، و"إعـداد ميـدان المعركة"، وأما الأفعال؛ من قبيل: اختراق شبكات الكهرباء في الـدول الأجنبيـة، بحيـث يمكن تعطيلها في زمن الحرب، فتؤدي إلى زعزعة الاسـتقرار، وزيـادة الاحـتمالات، بـأن

---

* البوتات أو روبوتات الشبكة العنكبوتية: تطبيقات براجمية تقوم بمهمات آلية على الإنترنت؛ ومنها: الهجمات المنسَّقة على الحواسيب الموصولة شبكياً. (المترجم)

** برامج يراد بها تدمير حواسيب متصفحي الإنترنت، أو سرقة بياناتهم. (المترجم)

*** رموز تُزرع عمداً، داخل نظم براجية، وتُطلِق وظائف خبيثة، عندما تتوافر شروط معينة. (المترجم)

**** برامج خبيثة، تبدو وكأنها تؤدي رغبة المستخدم، ولكنها تمهد الطريق؛ كي يصبح حاسوبه مستباحاً للدخول غير المأذون به. (المترجم)

يتسع نطاق الصراع في الفضاء الإلكتروني إلى العالم المادي، وعلى الولايات المتحدة، أن تسعى أيضاً، لتفادي أن تتحول الهجمات الإلكترونية إلى شكل خطير جديد، من أشكال الاحتجاج؛ أي مرحلة وسطى ما بين بذل المساعي [الدبلوماسية]، والقيام بردٍّ عسكري، وإذا أصبحت الهجمات الإلكترونية شكلاً مقبولاً من أشكال الاحتجاج الدولي، فإن آثار ذلك، قد تسهم بشكل خطير في زعزعة الاستقرار الاقتصادي، ويمكنها أن تفتح المجال أمام الصراعات العسكرية التقليدية.

والاتفاقات الدولية التي تقتضي منع اختراق شبكات الكهرباء، والقطاع المالي، والمكونات الأخرى للبنى الأساسية المدنية، قد تصب في مصلحة الولايات المتحدة، في نهاية المطاف، ولكنْ في المرحلة الحالية، نجد أن الدول في معظمها - ومنها الولايات المتحدة - غالباً ما لا ترغب في التخلي عن القيمة الاستخبارية المستقاة من استغلال تلك النظم، وعلى حكومة الولايات المتحدة، أن تشرع في عملية لاستبانة في أي ظروف ستخدم أو لا، تلك الاتفاقات، المصالح الأمريكية: (هشاشة تلك النظم، والتكلفة المرتبطة بحمايتها قد تفوق - في نهاية المطاف - المنافع المتحصَّل عليها من استغلال نظم الخصم)، وبينما قد يكون هذا الاقتراح، من السابق لأوانه أن يحظى بالدعم الكافي، من الحكومة الأمريكية والحكومات الأجنبية، فإن ثمة مجالين جاهزين؛ كي يتم التوصل إلى اتفاق دولي بشأنهما؛ للحد من تدخّل الدولة في الفضاء الإلكتروني، وفي كل مجال منهما، لا توجد مصالح استخبارية مهددة، وعلى الولايات المتحدة أن تضع اقتراحات للمعالجة المنفصلة لمسألتي الأمن والحرمة للعمليات الأساسية التي تتيح عمل الإنترنت، ولحظر هجمات حجب الخدمة.

الاعتراف بالجذر بوصفه قيمة استراتيجية دولية

كان الجذر root، في صلب حوكمة الإنترنت، منذ استحداث نظام اسم النطاق في ثمانينيات القرن العشرين، والنظام يوفِّر الرابط الضروري بين أسماء النطاق التي يمكن البشر قراءتها؛ مثل: CFR.org: [اسم العنوان الشبكي لمجلس العلاقات الخارجية]، وعناوين بروتوكولات الإنترنت التي يمكن الأجهزة قراءتها؛ من قبيل: 66.40.21.148.

ويعتمد النظام على 13 خادماً رئيسياً؛ لتوفير معلومات موثوق بها، بالنسبة إلى النطاقات من المرتبة العليا؛ (مثل: .com و.net و.us و.jp،... إلخ)؛ لبدء عملية الاستجابة لطلب يتعلق بخادم صفحة شبكية أو بريد إلكتروني، وهناك جهود تُبذل؛ لتحسين أمن الجذر، لكن عمليات الجذر، ماتزال عرضة لمحاولات الاختراق، ولهجمات حجب الخدمة الموزَّعة، وحجب الخدمة الواسعة النطاق؛ ولأن المعلومات المتضمَّنة في ملف منطقة الجذر، هي - بطبيعتها - مفتوحة للعموم، فما من قيمة استخبارية يمكن جنيها من محاولة الوصول إلى خادم جذري، وأما التوصل إلى اتفاق يُعترف بالجذر؛ بوصفه قيمة استراتيجية دولية، لا يجوز للدول أن تسعى لتعطيلها، فسوف يصب في المصلحة الأمريكية، وقد يكون بمنزلة خطوة أولى، باتجاه الحدّ من التوترات في الفضاء الإلكتروني، وماتزال سيطرة الولايات المتحدة على الجذر، إحدى القضايا التي هي محلّ خلاف، وبينما كانت الرغبة الأمريكية في المحافظة على هذا الدور، نابعة من ضمان استمرار أداء الجذر لوظائفه، فقد يكون من مصلحة الولايات المتحدة، أن توجد آلية دولية، تتولى الإشراف على الجذر؛ بوصفه جزءاً من صفقة كبرى، بشأن حوكمة الإنترنت.

السعي لاتفاقية تحظر هجمات حجب الخدمة

إن التوصل إلى اتفاق لحظر هجمات حجب الخدمة، سيركز - على غرار اتفاق حماية الجذر - على مشكلة ضيقة، لا يعقِّدها جمع الاستخبارات، أما هجمات حجب الخدمة فهي - بطبيعتها - من الأسلحة البدائية التي لا تتطلب اختراق الشبكات، وإنما تعطيلها، وهي أيضاً، سلاح فتّاك، سبق أن استخدم في العمليات الإجرامية، وكذلك في الصراعات التي تنشب على مستوى الدول، وفي ثلاثة أمثلة على الأقل، ضلعت الحكومة والجيش في روسيا في هجمات لحجب الخدمة، أو شجّع كلاهما على ذلك، ضد دول أجنبية؛ فعطَّل هذا البنية الأساسية للإنترنت والخدمات المعتمدة عليها لدى الضحايا؛ ومن بين تلك الهجمات: الهجوم الذي وقع عام 2007، واستهدف أستونيا، وهجوم عام 2008؛ مستهدفاً جورجيا، وهجوم عام 2009، ضد قيرغيزستان، وخلافاً لاستغلال الشبكة الحاسوبية، وهو الذي يمكن استخدامه للتخريب أو التجسس، فإن هجمات

حجب الخدمة، لا يمكنها أن تساعد إلا على تخريب أحد النظم؛ ومن هنا، فإن على الولايات المتحدة، أن تروِّج لاتفاقية من شأنها، إلزام الأطراف الموقِّعين بسياسة، يتم – وفقها – الحدّ من هجمات حجب الخدمة، خارج نطاق الصراعات التقليدية، ومنع تلك الهجمات بمقتضى معاهدة دولية، يمكن أن يكون الخطوة الأولى؛ لتأسيس المسؤولية في الفضاء الإلكتروني؛ ذلك أن هجمات حجب الخدمة في معظمها، ينفِّذها مجرمون؛ لأغراض الابتزاز، والمساعدة التي تقدمها الدول؛ لإحباط هجوم موزَّع لحجب الخدمة، يمكن استخدامها؛ للحكم على كون الدولة قد غضَّت الطرف عن الهجوم، أو أنه وقع ضد رغبتها، وإذا ساعدت الدول على وقف الهجوم، فعندئذٍ يجب التعامل وإياه؛ بوصفه عملاً إجرامياً، وإذا لم تستجب الدول كذلك، فإن ذلك سوف يجب أن يُفهم، على أنه إشارة إلى موافقة رسمية على الهجوم، وأن يعامَل – من ثم – بوصفه عملاً عدائياً.

وضع الأجندة التقنية

ظلَّ تركيز الأوساط التقنية للإنترنت، حتى وقتنا الحاضر، منصباً على التبادلية؛ أي قابلية تبادل المعلومات، ومع استمرار تطوّر التكنولوجيات التي تتيح عمل الإنترنت، فإن هناك حاجة إلى أن يُحوَّل ذلك التركيز نحو الأمن؛ فالتكنولوجيات الأساسية للإنترنت، كانت مصممة لشبكة مغلقة، يخضع فيها الدخول للسيطرة المحكمة، ويحظى جميع المستخدمين بالثقة بهم، ولم تكن تلك التكنولوجيات مستحدَثة، أو مصممة للأغراض التي تُستخدم الآن من أجلها، وهذه المشكلة – وهي التي تدركها الأوساط التقنية منذ زمن – ماتزال بانتظار المعالجة، وقد حددت "الوثيقة الوطنية الأمريكية لتأمين الفضاء الإلكتروني" لعام 2003، مكامن الضعف، ضمن ثلاثة من "بروتوكولات الإنترنت الرئيسية"؛ وهي: بروتوكول الإنترنت، ويُسترشد به في توجيه البيانات من المصدر إلى الوجهة المقصودة عبر الإنترنت، ونظام اسم النطاق، وهو يحوِّل أرقام بروتوكول الإنترنت إلى عناوين شبكية، يمكن التعرف إليها، وبروتوكول البوابة الحدودية، وهو الذي يوفِّر الاتصال بين الشبكات؛ لإيجاد "شبكة الشبكات"،[20] ولا يوجد في أي من تلك البروتوكولات آلية مدمجة؛ للتحقق من الأصل أو صحة المعلومات المرسلة إليها؛ بما

يعرِّضها للاحتيال أو التلاعب، من الأطراف السيِّئي النية، وقد أقرّت استراتيجية عام 2003، تلك المشكلات؛ ولكنها خلصت إلى أن «الصناعة الخاصة، تقود الجهد الذي يضمن تطوّر الوظائف الرئيسية للإنترنت، على نحو آمن»، وقصرت دور الحكومة الاتحادية، على تنسيق «الشراكات القائمة بين القطاعين العام والخاص؛ لتشجيع... اعتماد بروتوكولات أمن محسَّنة»،[21] وبعد مضي نحو عقد، ماتزال الإنترنت تعاني المشكلات ذاتها، وفي هذه المرحلة، يمكن الخلوص - بثقة - إلى أن نموذجي "التنسيق"، و"التشجيع"، لما يؤتيا بعدُ النتائج المرجوة، وهناك حاجة إلى أن تتحلى الحكومة الاتحادية بمستوى قيادة أقوى.

وتستطيع الولايات المتحدة - من خلال التحلّي بالقيادة، وتقديم المساعدة التقنية والتمويل - أن تعزِّز التطوير والاعتماد لمجموعة جديدة من البروتوكولات الآمنة التي ستعالج الكثير من مكامن الضعف في البنية الحالية للإنترنت، وتمنع - في الوقت ذاته - التطوير والاعتماد لبروتوكولات، تفرط في التوجه نحو استحداث دولة مراقبة على الإنترنت، أو نشوء خطر تفكك الإنترنت، إلى سلسلة من الشبكات الوطنية المبلقنة، [نسبة إلى البلقان]، والمنفصلة؛ والهدف - كما كتب ماركوس ساكس - هو تفادي نشوب "حرب باردة تقنية"، تطوِّر خلالها الولايات المتحدة والصين وأوربا: «شبكات حاسوبية مختلفة تقنياً، وغير قابلة للتشغيل المتبادل؛ على أساس بروتوكولات وقواعد، تتناسب وقيم كل مجتمع وأخلاقياته ونظمه القانونية».[22]

توجيه مؤسسة العلوم الوطنية لوضع تحدٍّ تقني أمام فرقة العمل المعنية بهندسة الإنترنت لوضع بروتوكولات آمنة

إن الطريقة المثلى لاستباق هذه النتيجة، هي المساعدة على استحداث مجموعة من البروتوكولات التي تبدِّد الهواجس الأمنية، على الوجه الكافي، من دون تفكيك الإنترنت، أو تحويلها إلى منصة عالمية للسيطرة الحكومية؛ فطوال أكثر من عقدين، قادت فرقة العمل المعنية بهندسة الإنترنت، تطوير المعايير التقنية التي تتيح للإنترنت أن تؤدي وظائفها، والفرقة وأعضاؤها، مجتمع مفتوح من الخبراء التقنيين من مختلف أنحاء العالم، قاد تطوّر

الإنترنت على مدى جيل، ويجب أن يُمنح الفرصة لمعالجة أوجه القصور الأمني التي تحيط بالشبكة الحالية، ويجب على حكومة الولايات المتحدة، أن تضع - بالتنسيق بينها وبين حلفائها - أمام الفرقة، التحدي الممثل باستحداث مجموعة جديدة من البروتوكولات الأكثر أمناً؛ والهدف - وهو الذي كان جون مايكل "مايك" ماكونل، المدير السابق للاستخبارات الوطنية، أبلغ المعبّرين عنه - يجب أن يمثل بـ «إعادة تصميم الإنترنت، بحيث تزداد القدرة على: إدارة الإسناد والموقع الجغرافي وتحليل الاستخبارات وتقويم الأثر - أي [الإجابة على الأسئلة]: من الفاعل؟ ومن أين؟ ولماذا؟ وما النتيجة؟»،[23] ولكنْ لا يجوز لها أن تسعى لأن تدمج في رموز الإنترنت الأساسية، إسناداً تاماً، يكون هو الأداة النهائية لدولة المراقبة.

وعلى مؤسسة العلوم الوطنية، أن تقود الجهد؛ لبلورة التحدي التقني، على أن يتم ذلك بالتنسيق بينها وبين الوكالات الاتحادية المعنية، والقطاع الخاص، والمؤسسات الأكاديمية، ويجب أن تركز المرحلة الأولية، على تحديد المشكلات الناجمة عن انعدام الأمن في الإنترنت، واستبانة: هل من الممكن معالجة تلك المشكلات، من خلال استحداث معايير تقنية جديدة أو لا؟ وكيف يتم ذلك؟ وعلى المؤسسة أن تنتقل - بعد ذلك - إلى طرح التحدي، والإشراف على نظام من المنح المقدمة، عن طريق فرقة العمل المعنية بهندسة الإنترنت، ويجب أن يتضمن التحدي، موعداً نهائياً يحلّ بعد أربع سنوات؛ لتقديم مجموعة من البروتوكولات الآمنة، والشروع في تنفيذها، ويجب أن يوضَّح - لدى تقديم التحدي - أن عدم الالتزام بالموعد النهائي، سينجم عنه استهلال مجهود اتحادي؛ لاستحداث بروتوكولات جديدة، وعلى الولايات المتحدة، أن تموِّل ذلك النشاط، وأن تسعى لنيل دعم دول أخرى، تتفق والنهج؛ كما صيغ، وكما عبِّر عنه؛ لضمان أن يستجاب للتحدي، وأن تتسق البروتوكولات المستحدثة والأهداف الشاملة للولايات المتحدة؛ لتطوير الفضاء الإلكتروني، وبعد ذلك، يجب توفير الحوافز التي ستساعد على تنفيذ تلك الأهداف.

تنظيم الجهد الأمريكي

تعكف القيادة الإلكترونية، على دمج الوحدات الإلكترونية، في: الجيش والبحرية وسلاح الجو والمارينز الأمريكي، ضمن جهد منسق؛ لحماية شبكات وزارة الدفاع، ودعم المهمات البرية والبحرية والجوية، وتنفيذ عمليات هجومية في الفضاء الإلكتروني، عندما تصدر لها الأوامر بذلك، والتشريع الذي ينظر فيه مجلس الشيوخ، سيعهد إلى وزارة الأمن الوطني، مهمة تأمين جميع النظم الحكومية المدنية، ويمنحها صلاحيات إضافية؛ لتنظيم البنى الأساسية الحساسة، في القطاع الخاص، توخياً للأمن الإلكتروني، وهناك ضرورة لجهد موازٍ؛ لضمان أن تكون الجهود الدبلوماسية، مع الدول الأجنبية - ضمن ملتقيات حوكمة الإنترنت - منسَّقة، وحائزة على الموارد اللازمة، وساعية لتحقيق أهداف أمريكية محددة.

تعيين نائب منسق البيت الأبيض للأمن الإلكتروني لحوكمة الإنترنت

في عهد إدارة بيل كلينتون، وُلِّيت موظفة واحدة، وهي آيرا ماجازينر، فعلياً، إدارة وضع سياسة حوكمة الإنترنت، والتواصل ومنتديات حوكمة الإنترنت، وقد اتسع نطاق المسألة كثيراً، بحيث لم يعد يمكن شخصاً واحداً أن يديرها بفعالية وحده، ولكنْ، لا بد أن يضطلع البيت الأبيض، بدور الريادة، إزاء ما يخصّ حوكمة الإنترنت؛ لتنسيق رسم السياسات، والإشراف على تنفيذها، والتشريع الذي من شأنه توسيع نطاق الصلاحيات الممنوحة لوزارة الأمن الوطني، سيكفل كذلك، أن يُنشأ - ضمن المكتب التنفيذي للرئيس - مكتب سياسات الفضاء الإلكتروني؛ على أن يناط به، الدور القائم لمنسق الأمن الإلكتروني، مع تعزيز ما لذلك المنصب، من صلاحية وميزانية وموظفين، ويجب أن يكون لمدير هذا المكتب، نائب لتنسيق السياسات الأمريكية، في مجال حوكمة الإنترنت، إلى جانب موظفين، يتولون الإشراف، بشكل يضمن النهوض بالأجندة الأمريكية، في مجال الفضاء الإلكتروني، في كل فرصة.

إنشاء مكتب جديد للشؤون الإلكترونية في وزارة الخارجية

لا بد من إعادة تنظيم وزارة الخارجية، وتزويدها بالموظفين؛ سعياً لتنفيذ الأجندة الأمريكية، في مجال الفضاء الإلكتروني، بحيث يتم التركيز - أساساً - على تأمين النطاق،

في جميع الملتقيات والعلاقات الثنائية التي تتعلق بالفضاء الإلكتروني، وعلى الرغم من أن وزارة الخارجية، تركز بإفراط في المرحلة الحالية، على مسألة حرية الإنترنت، بشكل يلحق الضرر بالأمن الإلكتروني، فإن ذلك الانحياز، يمكن تصحيحه، من خلال تكليف الوزارة بمهمة واضحة، إزاء ما يتعلق بحوكمة الإنترنت، بما يحقق التوازن بين المصالح التي تبدو متنافسة في ظاهرها، ومن خلال تزويد المؤسسة، بما تحتاج إليه من الموظفين من ذوي الدراية والخبرة، ويجب – على أقل تقدير – أن يكون لدى وزارة الخارجية، الموارد اللازمة؛ لتنسيق المواقف، عبر جميع فروع الحكومة، ومصاحبة الوفود كافة، كما يجب استحداث وظائف بدوام كامل، أو نقاط اتصال تابعة للوزارة، لدى الوكالات الأخرى ذات الصلة بذلك، والاستثمار المطلوب ضئيل نسبياً، لكن المنافع ستكون هائلة.

وبعد أن تم تأكيد أن الجنرال كيث ألكسندر، سيترأس القيادة الإلكترونية، وترقيته إلى رتبة جنرال ذي أربعة نجوم، فإن جهود وزارة الدفاع، في مجال الفضاء الإلكتروني، أصبح يقودها المسؤول الذي يحلّ في المرتبة الخامسة عشرة، على سلم التدرج الوظيفي بالوزارة، ومع إنشاء القيادة الإلكترونية، ضمن وزارة الدفاع، ينبغي منح مسألة الدبلوماسية الإلكترونية في وزارة الخارجية، الدرجة نفسها من الأهمية؛ وتحقيقاً لذلك، فإن على الكونجرس، أن يستحدث مكتباً للشؤون الإلكترونية، يتبع وكيل وزارة الخارجية للشؤون السياسية، وتكون من مهماته، الإشراف على: مؤسسات وزارة الخارجية المسؤولة – حالياً – عن مسائل الاتصالات الدولية، وحرية الإنترنت، والأمن الإلكتروني، وتشمل تلك المؤسسات: مكتب الشؤون الإلكترونية في الاستخبارات والبحوث، وهو المسؤول عن تحليل المسائل ذات الصلة بالأمن الإلكتروني، والتنسيق بين الوكالات والشؤون الدولية، والمجموعة المعنية بسياسات الاتصالات والمعلومات، ضمن مكتب شؤون الاقتصاد والطاقة والأعمال، وفرقة العمل المعنية بالحرية العالمية للإنترنت.

استحداث منتدى مركزي للقطاع الخاص لتنسيق أجندات حوكمة الإنترنت مع الحكومة الأمريكية

ينبغي لمكتب الشؤون الإلكترونية الجديد، أن يضمّ – كذلك – اللجان الاستشارية القائمة، ضمن وزارة الخارجية، إزاء ما يخصّ تكنولوجيا المعلومات؛ ومن ذلك: اللجنة

الاستشارية حول سياسات الاتصالات والمعلومات الدولية، واللجنة الاستشارية للاتصالات الدولية، وعلاوة على ذلك، لا بد من تشكيل لجنة جديدة، تركز - تحديداً - على الأمن الإلكتروني، وينبغي أن يخدم مكتب وحيد، تلك اللجان، بحيث يوفر منتدى مركزياً للقطاع الخاص؛ كي ينسق أجندات حوكمة الإنترنت، مع الحكومة الأمريكية، وتُعَدّ الشركات الأمريكية؛ من قبيل: مايكروسوفت، وسيمانتك، من الفاعلين المهمين في منتديات حوكمة الإنترنت، وفي الوقت الحاضر، نجد أن تلك الشركات، تتحمل جزءاً كبيراً من الحمل، وتفتقر إلى توجه واضح، بشأن كيفية النهوض بالمصالح القومية للولايات المتحدة، ومع أن مواقف الشركات الأمريكية، لا تتناسق وموقف الحكومة دائماً، فإن تلك الشركات، يجب أن تتاح لها الفرصة - مع ذلك - كي تشكل ذلك الموقف، وتفهم الأجندة التي تدعو الحكومة الأمريكية إليها.

زيادة التمويل للتواصل ومنتديات حوكمة الإنترنت

إن تعيين مسؤول كبير في البيت الأبيض؛ لشؤون حوكمة الإنترنت، واستحداث مكتب جديد، داخل وزارة الخارجية؛ لإدارة هذه القضية، لا يعنيان أن الوكالات الأخرى، ليس لها مصلحة، أو أنها لا يجوز أن تضطلع بدور، في التواصل الدولي، بشأن حوكمة الإنترنت، بل على العكس؛ فوزارات: الدفاع، والتجارة، والعدالة، والأمن الوطني - وكذلك: كيانات تابعة للوزارات؛ مثل: الإدارة الوطنية للاتصالات والمعلومات، ومكتب التحقيقات الاتحادي - ستواصل العمل، ضمن شراكات نشيطة: متعددة الأطراف وثنائية، ولكنها ستفعل ذلك، ضمن نظام، ينهض بجدول العمل الشامل للولايات المتحدة، ولا بد أن تكون مكاتبها المعنية بالشؤون الدولية، أو الكيانات المتواصلة ومنتديات حوكمة الإنترنت، مزودة بما يناسبها من الموظفين ذوي المستوى العالي الكافي، وأن يكون لديها: الوقت والموارد؛ للاستعداد للتواصل، وفي الوقت الراهن، فإن حوكمة الإنترنت، ليست من الأعمال التي يمكن الجميع امتهانها.

الخاتمة

إن الإنترنت تقف عند نقطة حاسمة، في تاريخها القصير نسبياً؛ فالأعمال الشريرة التي يقوم بها المجرمون والجواسيس والمحاربون، تهدد النمو والكفاءة الاقتصاديين اللذين تمخض عنهما، وجود شبكة عالمية وحيدة وتبادلية، وإذا لم تتم معالجة تلك التهديدات، على نحو بنّاء، من خلال مشاركة أمريكية ذات نطاق أوسع، فإن دولاً أخرى، ستدخل الساحة، وقد تصوغ حلاً، من شأنه: حرمان الإنترنت من الخصائص ذاتها التي أكسبتها القيمة في المقام الأول؛ وبأخذ تلك العوامل في الحسبان، فإن على الولايات المتحدة أن تتجاوز معارضتها التقليدية للتواصل، إزاء ما يتعلق بمسائل حوكمة الإنترنت، وأن تقود الجهود بين الدول ذات التوجهات المتشابهة؛ لتبديد الهواجس الأمنية؛ بوسائل من شأنها: تعزيز الإنترنت؛ بوصفها محركاً للنمو الاقتصادي، لا الانتقاص منها، وعلى الولايات المتحدة، أن تعمل على استحداث آليات دولية جديدة؛ لوقف الهجمات الإلكترونية، وملاحقة منفِّذي تلك الهجمات، وكبح الدول الضالعة في النشاط الضار؛ وهذه الجهود - إلى جانب الاستثمارات الرامية إلى إعادة هيكلة البروتوكولات الأساسية للإنترنت؛ لجعلها أكثر أمناً - يمكن أن تحفظ القيمة الاقتصادية المستقاة، من الإنترنت، وتوسِّع نطاقها.

الهوامش

1. انظر:

"Unsecured Economies: Protecting Vital Information," McAfee, January 21, 2009, http://www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html.

2. انظر:

Virtually Here: The Age of Cyber Warfare, McAfee Virtual Criminology Report, 2009, p. 13.

3. انظر:

Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, October 21, 2007.

4. انظر:

Stewart Baker, Shaun Waterman, and George Ivanov, *In the Crossfire: Critical Infrastructure in the Age of Cyber War* (Santa Clara, CA: McAfee, 2010).

5. بحسب تعريف القانون الاتحادي، فإن مصطلح "الإنترنت"، يشير إلى الشبكة الحاسوبية الدولية المكونة من شبكات بيانات اتحادية وغير اتحادية، قابلة للتشغيل المتبادل، وتعمل بتقنية تحويل الطرود: [أجزاء المعطيات الرقمية المراد نقلها] packet switching.

6. انظر:

Jeremy Malcolm, *Multi-stakeholder Governance and the Internet Governance Forum* (Perth: Terminus Press, 2008), p. 32.

7. «يدعو إعلان سلفادور، إلى إصلاح العدالة الجنائية؛ لتأمين حقوق الإنسان والأمن والتنمية»، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 19 نيسان/ إبريل 2010. انظر الموقع الشبكي:

http://www.unodc.org/southerncone/en/frontpage/2010/04/19-declaracao-de-salvadorpede-uma-reforma-da-justica-criminal-para-proteger-os-direitos-humanos-aseguranca-e-o-desenvol vimento.html.

8. انظر:

UN System Chief Executives Board for Coordination, First Regular Session of 2010, UNIDO Headquarters, Vienna, April 9, 2010, pp. 11-12.

9. انظر:

"Connecting America: The National Broadband Plan," Federal Communications Commission, March 15, 2010, p. xi, http://download.broadband.gov/plan/national broadband-plan.pdf.

10. للاطلاع على نقاش معمّق حول هذه المسألة، انظر:

Robert K. Knake, "Untangling Attribution: Moving to Accountability in Cyberspace," testimony before the House of Representatives Committee on Science and Technology, July 15, 2010, http://www.cfr.org/publication/22630/untangling_attribution.html.

11. هذا المفهوم، طوَّره جيسون هيلي، من رابطة دراسات الصراعات الإلكترونية، في:

"Beyond Attribution: A Vocabulary for National Responsibility for Cyber Attacks," April 1, 2010, http://www.cyberconflict.org/ccsa-in-the-news/jasonhealeyslatestpaper.

12. انظر:

"Cybercrime Convention: A Positive Beginning to a Long Road Ahead," *Journal of High Technology Law*, vol. 2, no. 1, 2003, p. 110.

13. انظر:

Council of Europe, "Convention on Cybercrime," CETS No. 185, July 1, 2004, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

14. انظر:

Financial Action Task Force, "About the Financial Action Task Force," http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1_1,00.html.

15. للاطلاع على نبذة عامة عن فرقة العمل المعنية بالعمل المالي، انظر:

"An Introduction to FATF and Its Work," FATF-GAFI, 2010, http://www.fatf-gafi.org/dataoecd/48/11/45139480.pdf.

16. للاطلاع على المزيد من المعلومات، حول مجموعة أدوات الاتحاد الدولي للاتصالات، بشأن تشريعات الجريمة الإلكترونية، انظر:

"ITU Cybercrime Legislation Resources: ITU Toolkit for Cybercrime Legislation," International Telecommunications Union, http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html.

17. انظر:

Oxford Internet Institute, "Mapping and Measuring Cybercrime (Invited Forum)," University of Oxford, January 22, 2010, http://www.oii.ox.ac.uk/events/?id=337.

18. ينظر مجلس الشيوخ الأمريكي، في اعتماد نهج أحادي، ويقضي قانون الإبلاغ عن الجريمة الإلكترونية الدولية والتعاون بشأنها، أن يقدِّم الرئيس تقويماً سنوياً، حول الجريمة الإلكترونية الدولية، وأن يعلِّق المساعدات والتمويل والبرامج التجارية؛ على أساس تلك النتائج، ولمشروع القانون، وهو الذي

اشترك في تقديمه، كلٌّ من: كيرستن جيليبراند (السيناتورة الديمقراطية عن نيويورك)، وأورين هاتش (السيناتور الجمهوري عن يوتا)، ميزاته، ولكنه يخفق في أحد الجوانب المهمة؛ فهو لا يقوِّم أحد أكبر ملاذات مجرمي الإنترنت - أي الولايات المتحدة - بما يقلِّص احتمال أن يكون له التأثير الفاضح المطلوب، وعلاوة على ذلك، فإن أي عقوبات تفرضها الولايات المتحدة؛ بناءً على تلك التصنيفات، لا يُحتمل أن يكون لها التأثير المطلوب، في الدول المستهدفة، من حيث تحسّن سلوكها.

19. انظر:

Richard Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010).

20. انظر:

The White House, *The National Strategy to Secure Cyberspace*, February 2003, p. 30.

21. Ibid.

22. انظر:

Marcus H. Sachs, *Who e-Governs?* George Mason University, Policy Analysis Research Paper, December 4, 2007, p. 14.

23. انظر:

"Mike McConnell on How to Win the Cyber War We're Losing," *Washington Post*, February 28, 2010.

قواعد النشر

أولاً: القواعد العامة

1. تقبل للنشر في هذه السلسلة البحوث المترجمة من اللغات الأجنبية المختلفة، وكذلك الدراسات التي يكتبها سياسيون وكتاب عالميون.
2. يُشترط أن يكون البحث المترجم أو الدراسة في موضوع يدخل ضمن اهتمامات المركز.
3. يشترط ألا يكون قد سبق نشر الدراسة أو نشر ترجمتها في جهات أخرى.
4. تصبح الدراسات والبحوث المنشورة في هذه السلسلة ملكاً لمركز الإمارات للدراسات والبحوث الاستراتيجية، ولا يحق للمترجم أو المؤلف إعادة نشرها في مكان آخر.
5. يتولى المركز إجراءات الحصول على موافقة الناشرين الأصليين للبحوث المترجمة.

ثانياً: إجراءات النشر

1. تقدم الدراسة أو الترجمة مطبوعة من نسخة واحدة.
2. ترفق مع الترجمة صورة من المقالة باللغة المترجم عنها، وبيانات عن المصدر الذي أخذت منه.
3. يرسل مع البحث أو الترجمة بيان موجز بالسيرة العلمية للمترجم أو للباحث.
4. تقوم هيئة التحرير بمراجعة البحث أو الترجمة للتأكد من مستواهما، من خلال مراجعين من ذوي الاختصاص.
5. يخطر الباحث أو المترجم بنتيجة المراجعة خلال ثلاثة أشهر من تاريخ تسلم البحث.
6. تتولى هيئة التحرير المراجعة اللغوية وتعديل المصطلحات بما لا يخل بمضمون البحث أو الترجمة.

صدر من سلسلة «دراسات عالمية»

	العنوان	المؤلف
1.	نحو شرق أوسط جديد، إعادة النظر في المسألة النووية	أفنر كوهين
2.	السيطرة على الفضاء في حرب الخليج الثانية وما بعدها	ستيفن لمباكيس
3.	النزاع في طاجكستان، التفاعل بين التمزق الداخلي والمؤثرات الخارجية (1991 - 1994)	جوليان ثوني
4.	حرب الخليج الثانية، التكاليف والمساهمات المالية للحلفاء	ستيفن داجت جاري جي. باجليانو
5.	رأس المال الاجتماعي والاقتصاد العالمي	فرانسيس فوكوياما
6.	القدرات العسكرية الإيرانية	أنتوني كوردزمان
7.	برامج الخصخصة في العالم العربي	هارفي فيجنباوم وجفري هينج وبول ستيفنز
8.	الجزائر بين الطريق المسدود والحل الأمثل	هيو روبرتس
9.	المشكلات القومية والعرقية في باكستان	أبها دكسيت
10.	المناخ الأمني في شرق آسيا	سنجانا جوشي
11.	الإصلاح الاقتصادي في الصين ودلالاته السياسية	وي وي زانج
12.	السياسة الدولية في شمال شرق آسيا... المثلث الاستراتيجي: الصين - اليابان - الولايات المتحدة الأمريكية	توماس ويلبورن
13.	رؤية استراتيجية عامة للأوضاع العالمية	إعداد: إيرل تيلفورد
14.	العراق في العقد المقبل: هل سيقوى على البقاء حتى عام 2002؟	جراهام فولر
15.	السياسة الخارجية الأمريكية بعد انتهاء الحرب الباردة	دانيال وارنر
16.	التنمية الصناعية المستديمة	ديفيد والاس
17.	التحولات في الشرق الأوسط وشمال إفريقيا: التحديات والاحتمالات أمام أوربا وشركائها	فيرنر فاينفلد ويوزيف ياننج وسفن بيرنيد
18.	جدلية الصراعات العرقية ومشروعات النفط في القوقاز	فيكن تشيتريان
19.	العلاقات الدفاعية والأمنية بين إنجلترا وألمانيا «نظرة تقويمية»	إدوارد فوستر وبيتر شميت

صدر من سلسلة «دراسات عالمية»

صدر من سلسلة «دراسات عالمية»

العنوان	المؤلف
35. دولة الإمارات العربية المتحدة الوطنية والهوية العربية - الإسلامية	سالي فندلو
36. استقرار عالم القطب الواحد	وليم وولفورث
37. النظام العسكري والسياسي في باكستان	تأليف: إيزابيل كوردونير ترجمة: عبدالله جمعة الحاج
38. إيران بين الخليج العربي وحوض بحر قزوين الانعكاسات الاستراتيجية والاقتصادية	شيرين هنتر
39. برنامج التسلح النووي الباكستاني نقاط التحول والخيارات النووية	سمينة أحمد
40. تدخل حلف شمال الأطلسي في كوسوفا	ترجمة: الطاهر بوساحية
41. الاحتواء المزدوج وما وراءه: تأملات في الفكر الاستراتيجي الأمريكي	عمرو ثابت
42. الصراع الوطني الممتد والتغير في الخصوبة: الفلسطينيون والإسرائيليون في القرن العشرين	فيليب فرج
43. مفاوضات السلام وديناميكية الصراع العربي - الإسرائيلي	عمرو جمال الدين ثابت
44. نفط الخليج العربي: الإنتاج والأسعار حتى عام 2020	ديرموت جيتلي
45. انهيار العملية السلمية الفلسطينية - الإسرائيلية: أين الخلل؟	جيروم سليتر
46. ثورة المعلومات والأمن القومي	تحرير: توماس كوبلاند
47. القانون الدولي والحرب ضد الإرهاب	كريستوفر جرينوود
48. إيران والعراق	تشاس فريمان (الابن) وآخرون
49. إصلاح نظم حقوق الملكية الفكرية في الدول النامية: الانعكاسات والسياسات	طارق علما ومايا كنعان
50. الأسطورة الخضراء: النمو الاقتصادي وجودة البيئة	ماريان رادتسكي

صدر من سلسلة «دراسات عالمية»

.51	التصورات العربية لتركيا وانحيازها إلى إسرائيل بين مظالم الأمس ومخاوف اليوم	أوفرا بنجيو وجنسر أوزكان
.52	مستقبل الأيدز: الحصيلة المروعة في روسيا والصين والهند	نيكولاس إيبراشتات
.53	الدور المتغير للمعلومات في الحرب	تحرير: زلمي خليل زاد وجون وايت
.54	مسؤولية الحماية وأزمة العمل الإنساني	جاريث إيفانز ومحمد سحنون وديفيد ريف
.55	الليبرالية وتقويض سيادة الإسلام	عمرو ثابت
.56	الوفاق الهندي - الإسرائيلي	أفرايم إنبار
.57	الفضائيات العربية والسياسة في الشرق الأوسط	محمد زياني
.58	دور تصدير المياه في السياسة الإيرانية الخارجية تجاه مجلس التعاون لدول الخليج العربية	كامران تارمي
.59	أهمية النجاح: الحساسية إزاء الإصابات والحرب في العراق	كريستوفر جيلبي وآخران
.60	الفوز مع الحلفاء: القيمة الاستراتيجية للنموذج الأفغاني	ريتشارد أندريس وآخران
.61	الخروج من العراق: استراتيجيات متنافسة	توماس ماتير
.62	آراء من داخل الشبكة: تأثير المواقع الإلكترونية في الاهتمامات السياسية للشبان	آرثر لوبيا و تاشا فيلبوت
.63	دبلوماسية الصين النفطية في إفريقيا	أيان تايلر
.64	التدخل العسكري والأسلحة النووية: حول المبدأ الأمريكي الجديد بشأن استخدام السلاح النووي	هارالد مولر و شتيفاني زونيوس ترجمة: عدنان عباس علي
.65	العقوبات في السياسة الدولية: نظرة على نتائج الدراسات والأبحاث	بيتر رودولف ترجمة: عدنان عباس علي
.66	اللوبي الإسرائيلي والسياسة الخارجية الأمريكية	جون ميرشايمر وستيفن والت

صدر من سلسلة «دراسات عالمية»

العنوان	المؤلف
67. نهوض الهند	جورشاران داس سي. راجا موهان أشتون بي كارتر سوميت جانجولي
68. التكاليف الاقتصادية لحرب العراق	تأليف: ليندا بيلمز جوزيف ستيجليتز ترجمة: عمر عبدالكريم الجميلي
69. إيران النووية: الانعكاسات وطرائق العمل	تأليف: إفرايم كام ترجمة: ثروت محمد حسن
70. حروب الخليج: مراجعات للسياسة الأمريكية تجاه العراق وإيران	جيمس فيرون راي تقيه
71. هل يُكرَّر سيناريو مفاعل تموز؟ تقويم القدرات الإسرائيلية على تدمير المنشآت النووية الإيرانية	ويتني راس و أوستن لونج ترجمة: الطاهر بوساحية
72. رؤيتان للسياسة الخارجية الأمريكية: جمهورية وديمقراطية	رودولف جولياني و جون إدواردز
73. مقاربات غربية للمسلمين في الغرب وللإسلام السياسي	بول ويلر وروبرت ليكن وستيفن بروك
74. الدولار واليورو هل يحتم العجز الكبير في ميزان الحساب الجاري الأمريكي ارتفاعاً في قيمة اليورو؟	يوناس دوفيرن كارستن باتريك ماير يوآخيم شايده ترجمة: عدنان عباس علي
75. القفزة الكبرى إلى الوراء! تكاليف أزمة الصين البيئية	إليزابيث إكونومي
76. اتفاقيات التجارة الحرة الثنائية في منطقة آسيا - المحيط الهادي: إشكالياتها ونتائجها	هريبرت ديتر ترجمة: عدنان عباس علي

صدر من سلسلة «دراسات عالمية»

77. إعادة التفكير في المصلحة القومية واقعية أمريكية من أجل عالم جديد — كونداليزا رايس
78. الصين المتغيرة: احتمالات الديمقراطية في الداخل والدبلوماسية الجديدة تجاه "الدول المارقة" — جون ثورنتون وستيفاني كلين - ألبراندت وأندرو سمول
79. التوجه الجديد لليبيا — مولفريد بروت - هيجهامر ورونالد بروس سانت جون
80. أزمة الغذاء العالمية — ألكس إيفانز ويواخيم فون براون وآخرون
81. عهد أوباما سياسة أمريكية للشرق الأوسط — ريتشارد هاس ومارتن أنديك ووالتر راسل ميد
82. اللوبي الهندي والاتفاقية النووية الأمريكية - الهندية — جيسون أ. كيرك
83. وقت الإغلاق: التهديد الإيراني لمضيق هرمز — كيتلين تالماج
84. دور حكام الولايات في السياسة الخارجية الأمريكية — صامويل لوكاس ماكميلان
85. الأزمة المالية العالمية — بن ستيل وستيفن دوناواي
86. شرق إفريقيا: الأمن وإرث الهشاشة — جيلبرت خادياجالا
87. المتعاقدون في الحروب — مارك كانسيان وستيفن شونر
88. الثقافة الاستراتيجية الإيرانية والردع النووي — جنيفر كنيبر وأندرو تيريل
89. أمن الطاقة الأوراسية — جفري مانكوف
90. أسلحة الدمار الشامل والأسلحة الصغيرة والخفيفة: فرق عمل تعزيز القدرات الأمنية المتعددة الأطراف — معهد السلام الدولي
91. هل التقسيم حلٌّ للحرب الأهلية؟ — نيكولاس سامبانس وجونا شولهوفر-ول
92. الصراعات في أقاليم الصومال — سولومون ديرسو وبيروك مسفين

صدر من سلسلة «دراسات عالمية»

93. الغرب وروسيا في البحر الأبيض المتوسط: نحو تنافس متجدد!	ديريك لوتربيك وجورجي إنغلبريخت
94. ما بعد الدولار: إعادة التفكير في النظام النقدي الدولي	باولا سوباتشي وجون دريفل
95. حوكمة الإنترنت في عصر انعدام الأمن الإلكتروني	روبرت كنيك

قسيمة اشتراك في سلسلة

«دراسـات عالميـة»

الاسـم: ....

المؤسسة: ....

العنوان: ....

ص. ب: .... المدينـة: ....

الرمز البريدي: ....

الدولة: ....

هاتف: .... فاكس: ....

البريد الإلكتروني: ....

بدء الاشتراك: (من العدد: .... إلى العدد: ....)

رسوم الاشتراك*

للأفراد:	220 درهماً	60 دولاراً أمريكياً
للمؤسسات:	440 درهماً	120 دولاراً أمريكياً

- ❑ للاشتراك من داخل الدولة يقبل الدفع النقدي، والشيكات، والحوالات النقدية.
- ❑ للاشتراك من خارج الدولة تقبل فقط الحوالات المصرفية، مع تحمل المشترك تكاليف التحويل.
- ❑ في حالة الحوالة المصرفية، يرجى تحويل قيمة الاشتراك إلى حساب مركز الإمارات للدراسات والبحوث الاستراتيجية رقم 1950050565 ـ بنك أبوظبي الوطني ـ فرع الخالدية. ص. ب: 46175 أبوظبي ـ دولة الإمارات العربية المتحدة.
- ❑ يمكن الاشتراك عبر موقعنا على الإنترنت (www.ecssr.ae) باستعمال بطاقتي الائتمان Visa و Master Card.

لمزيد من المعلومات حول آلية الاشتراك يرجى الاتصال:

مركز الإمارات للدراسات والبحوث الاستراتيجية

قسم التوزيع والمعارض

ص.ب: 4567 أبوظبي ـ دولة الإمارات العربية المتحدة

هاتف: 4044445(9712) فاكس: 4044443(9712)

البريد الإلكتروني: books@ecssr.ae

الموقع على الإنترنت: http://www.ecssr.ae

* تشمل رسوم الاشتراك الرسوم البريدية، وتغطي تكلفة اثني عشر عدداً من تاريخ بدء الاشتراك.

مركز الإمارات للدراسات والبحوث الاستراتيجية

ص.ب: 4567 - أبوظبي - دولة الإمارات العربية المتحدة

هاتف: 4044541 -2- 971 - فاكس: 4044542 -2- 971

E-mail: pubdis@ecssr.ae

Website: http://www.ecssr.ae

ISSN 1682 - 1211

ISBN 978-9948-14-412-0

9 789948 144120